Falcon ver. 2.23
Guía del Usuario

Synel Industries Ltd.

Este manual fue emitido en 2006-01-29.
Número de Catálogo 659993 Documento no. (21-9991601-7)

Este documento fue preparado para *Falcon* ver. 2.23.

Copyright © 1998-2006 Synel Industries Ltd. Todos los derechos reservados. La reproducción o el uso del contenido editorial o ilustrado, sin el permiso expreso, es totalmente prohibido. No se asume ninguna responsabilidad de patente con respecto al uso de la información contenida aquí. Mientras se han tomado todas las precauciones en la preparación de este manual, Synel Industries Ltd. no asume ninguna responsabilidad por errores u omisiones. Ninguna responsabilidad es asumida por daños resultantes del uso de la información aquí contenida.

Falcon es una marca registrada de Synel Industries Ltd.

Todos los nombres comerciales referidos aquí son nombres comerciales o marcas registradas de sus respectivas compañías.

IBM PC es una marca registrada de IBM Corporation.

Windows es una marca registrada de Microsoft Corporation.

Índice

Capítulo 1 – Introducción 1
1.1 Requisitos del Sistema 1
1.2 Información General 1
1.3 Mejoras 2
1.3.1 Sobre la versión 2 2
1.3.2 Sobre la versión 2.13 2
1.3.3 Sobre la versión 2.15 2
1.3.4 Sobre la versión 2.16 2
1.3.5 Sobre la versión 2.18 3
1.3.6 Sobre la versión 2.20 3
1.3.7 Sobre la versión 2.22 3
1.4 Ediciones de Falcon 4

Capítulo 2 – Instalación 5
2.1 HASP – Enchufe de Protección 5
2.2 Software 6
2.3 Instalación para Usuarios Múltiples 6
2.4 Opciones de la línea de Comando del *Falcon* 7

Capítulo 3 – Configuración 8
3.1 Configurando el Sistema 8
3.2 Croquis del sistema 8
3.3 Parámetros Generales 9
3.3.1 Configuraciones Predeterminadas 9
3.3.2 Configuraciones del Sistema 10
3.3.3 Configuraciones de Comunicación 10
3.3.4 Configuraciones de Archivos y Directorios. 11
3.4 Herramientas 12
3.4.1 Opciones 12
3.4.2 Importar Archivos del Personal 17
3.4.3 Editar Distribución de la Tarjeta (solamente en la versión PRO) 18

Capítulo 4 –Personal 21
4.1 Definir parámetros para un nuevo empleado 22
4.1.1 Ficha de control de acceso 23
4.1.1.1 Administración 24
4.1.1.2 General… 24
4.1.1.3 Detalles 24
4.1.2 Sacar una Foto (solamente en la versión PRO) 24
4.1.3 Imprimir una Tarjeta (solamente en la versión PRO) 25
4.2 Departamento & Compañía 25
4.3 Grupos de Cálculo 25

Capítulo 5 – Operación de Rutina. 28
5.1 Calendario 28

5.2 Auto Modos....30
5.2.1 Auto Modo para terminales Master.. ..30
5.2.1.1 Lista Auto Modo....30
5.2.1.2 Lista de Detalles de Auto Modo....30
5.2.1.3 Definir Auto Modo... 30
5.2.2 Auto Modo para SY-400.... 31
5.3 Lista de Terminales..... 32
5.3.1 Definir un Terminal Master....32
5.3.2 Definir una Lectora de Acceso....33
5.3.3 Definir un Terminal SY-400....35
5.3.4 Definir una Lectora SY-400....39
5.3.5 Definir un Terminal COM-II-PRO....40
5.3.6 Definir un Controlador de Alarma (solamente en la versión PRO)....41
5.3.7 Definir un Detector de Alarma....41
5.4 Definir una Zona Horaria....41
5.4.1 Definir una Zona Horaria para un Terminal Master....41
5.4.2 Definir una Zona Horaria para el SY-400… 42
5.5 Definir un Grupo de Seguridad....43
5.6 Definir un Empleado....44

Capítulo 6 – Comunicación 45
6.1 Enviar datos al terminal. 45
6.2 Recuperar datos desde el terminal....46

Capítulo 7 – Eventos 47

Capítulo 8 – Traducción de Mensajes 49

Capítulo 9 – Informes 51
9.1 Informe de Presencia / Ausencia 52
9.2 Informe de Transacción 52
9.2.1 General… 52
9.2.2 Lectora / Grupo de Seguridad / Grupo de Cálculo /Selección de Población....54
9.3 Visitantes....55
9.3.1 General… 55
9.3.2 Lectoras 55
9.4 Eventos....55
9.5 Entradas....55
9.6 Sistema....56
9.7 Grupo de Seguridad del Personal....57
9.8 Lectoras por Grupo de Seguridad 57
9.9 Zonas Horarias de Acceso a las Lectoras....58
9.10 Repetidos....58
9.10.1 Tarjetas Repetidas....58
9.10.2 Nombres Repetidos....58
9.10.3 IDs Repetidas....58
9.10.4 Fotografías Repetidas 58
9.11 Generador....58

9.12 Informe Personalizado 59
9.13 Adicionales....59
9.13.1 Fecha Prescrita....59
9.13.2 Tarjetas Emitidas 59
9.13.3 Personal Activo para TimeLOG 59

Capítulo 10 –Trabajando en Línea 60
10.1 Administración de Eventos en Línea 61
10.2 Borrar la tabla en línea 62

Capítulo 11 –Visitantes 63
11.1 Creando Tarjetas vía Personal....63
11.2 Manejo de Visitantes....63

Capítulo 12 – Manutención 65

Capítulo 13 – Localización 67
13.1 Emergencia....67
13.1.1 Producir un Informe de Incendio (emergencia) 71
13.1.2 Control de la puerta 67

Capítulo 14 – Mapas 69

Capítulo 15 – Huellas Digitales 71
15.1 Hardware....72
15.1.1 Definiciones de SY-400....72
15.2 Software 72
15.2.1 Opciones del Sistema....72
15.2.2 Opciones Locales....73
15.2.3 Actividades del Empleado 73
15.3 Sincronizando Plantillas....74

Capítulo 16 – Terminología 75

Capítulo 17 – Solución de Problemas 76

Apéndice A – Integración CCTV (PRO) 77
Regard: Regard i y Regard Remote CS COM interfaz....77
NegeVision: VideoRemote....77
Pelco: G-Protocol matriz 77
Vicon: V1500 78

Apéndice B – Base de Datos 79
Archivos 79
Extensiones....80
Otros Archivos 80
Idiomas Extranjeros....81

Apéndice C – Actualización.... 82

Apéndice D – Utilidades.... 83

Apéndice E – Configuración de la Red Master 85
Procedimientos Telnet....85
Usando el Comando ARP....86

Apéndice F – Mensajes de Error 87

Apéndice G – Servidor SY..... 89
Definiciones del Servidor SY.....89
Definiciones Falcon.....90
Definiciones DLL.....90

Capítulo 1 - Introducción

1.1 Requisitos del sistema

- Procesador Intel Pentium o superior
- Microsoft Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP o Windows 2003.
- 128 MB de RAM
- 100 MB de espacio disponible en el disco duro
- Adaptador de presentación de 256-colores (8-bit), 800x600 (24-bit – recomendado completamente de color)
- Unidad de CD-ROM
- Tarjeta opcional de sonido recomendada para notificaciones de eventos
- Tarjeta de captura compatible con TWAIN o escáner solamente para la versión *Falcon* PRO

1.2 Información General

El manejo de un sistema de control de acceso con numerosas lectoras y usuarios múltiples es una tarea complicada, especialmente en un sistema dinámico, de constantes alteraciones, en el cual lectoras son añadidas y desplazadas y las definiciones de acceso cambian constantemente.

Falcon hace de esto una tarea fácil. Define grupos de acceso, en los cuales son insertadas las definiciones de todos los parámetros que pertenecen a los dominios de acceso limitado, según zonas horarias y fecha, atribuyendo una cantidad ilimitada de tarjetas de acceso (empleados) a cada grupo.

Después de una actualización simple de un grupo de acceso, se asigna a un empleado un nuevo sistema total de definiciones de acceso. Además, cuando una nueva lectora es añadida al sistema, es vinculada a un grupo de acceso, permitiendo acceso a todos los empleados dentro de ese grupo. A seguir presentamos una lista de los elementos básicos de este sistema:

Lectora – Una unidad que reconoce un código de tarjeta y la atribuye a un empleado. La lectora se comunica con el controlador y el controlador con el PC.

Controlador – Una unidad que administra las lectoras en el sistema.

Tipo de día – Una plantilla compatible con variantes de días de trabajo y de no-trabajo según las definiciones y requerimientos de la empresa.

Zona Horaria – Define una franja horaria en la cual el acceso es permitido. Las Zonas Horarias son tipos de días definidos para el periodo de un año.

Grupo de Seguridad – Un concepto abstracto definiendo las Lectoras y Zonas Horarias a las cuales los empleados son asignados para la finalidad de una fácil administración del sistema de control de acceso (Véase Croquis del Sistema en la página 8).

El símbolo siguiente será usado en este manual para indicar características no respaldadas por *Falcon Express* -

1.3 Mejoras

1.3.1 Sobre la versión 2

- **Personal:**
  Una imagen puede ser capturada del *Falcon 2.12*.
  Impresión de tarjetas.
- **Herramientas/Opciones:**
  Una pantalla para planear la tarjeta (definiciones para la impresión de la tarjeta).
- **Vínculo Configuración/Terminal:**
  Falcon PRO respalda el sistema CCTV de Regard.
  Campos del sitio del nombre de la cámara fotográfica añadidos a controladores y a lectoras.
- **Mapas:**
  Una nueva pantalla exhibe gráficamente la localización de los terminales.
- **General:**
  Opera mejor en un ambiente de usuarios múltiples.
- **Herramientas Externas:**
  Reindex.exe- Para regenerar los archivos de índice exteriores al *Falcon*.
  Falcupd.exe- Actualización de la base de datos de versiones anteriores.
- **Informes - adicionales:**
  Fecha de Caducidad
  Nombre Duplicado
  ID Duplicado
  Informe de Edición
  Informe de Entradas
  Grupo de Seguridad Personal

1.3.2 Sobre la versión 2.13

- **General:**
  Una nueva lectora SY-400 - PRX-30
  - **Personal: D** detalles del Empleado
- **Herramientas/Opciones:**
  Soporte para la verificación de huellas digitales
- **Mapas:**
  Dos separadas pantallas: Editar sitio y visualizar sitio permitiendo una administración más fácil del evento
- **Informes:**
  Eventos en abierto
  Tiempo de respuesta
  Eventos antiguos

1.3.3 Sobre la versión 2.15

- Modo Automático para SY-400
- Envío de actualizaciones a los terminales SY-400
- Velocidad substancialmente mejorada en la emisión de informes de Transacción y Presencia/Ausencia

1.3.4 Sobre la versión 2.16

- **Menú de Emergencia:**
  Un nuevo menú para actividades de emergencia.

- **Lista del Operador:**
  Nuevas permisiones para abrir/trabar puertas.
- **Opciones:**
  Todas las opciones de comunicación pueden ser bloqueadas para todas las computadoras.
- **Huellas Digitales:**
  - Es posible ahora enviar una plantilla de empleado a todos los terminales SY-400.
  - Número de huellas digitales por persona fue aumentado a 10.
- Una nueva ficha SMS contiene definiciones del modem para envío de SMS.
- **Importación Automática:**
  Campos adicionales opcionales.

1.3.5 Sobre la versión 2.18

- **Detalles del Empleado:**
  Una persona puede tener 5 grupos de seguridad
- **Importación Automática:**
  Campos adicionales y configuraciones opcionales.
- **Informes:**
  Informe del Personal del Grupo de Seguridad
  Informe de Ausencia
  Informe de Transacción con total
- **Lista de Terminales:**
  Controlador de alarma + detectores de alarma (solamente en la versión PRO).
- **Huellas Digitales**: Soporta plantilla de ID con 10 dígitos

1.3.6 Sobre la versión 2.20

- **Informes:**
  Informe **Transacción** muy elaborado.
  Informe Tarjetas Duplicadas
  Informe Fotografías Duplicadas
  Informe Lectoras por Grupo de Seguridad
  Informe Zonas Horarias de Lectoras de Acceso
- **Capturar firma**: una opción para trabajar con una almohadilla para firmas
- Respaldo para matrices Pelco y Vicon CCTV (solamente en la versión PRO)
- **Huellas Digitales**: respaldo para trabajar con unidades de Identificación y FPU-S
- **Importación automática**: configuraciones adicionales
- **Terminal Master**: Escribir con listas no en línea

1.3.7 Sobre la versión 2.22

- **Detalles del Empleado**: Un nuevo botón **Add Trans**, para añadir transacciones manualmente
- **Grupo de Cálculo**: Para administrar centros de costo
- **Departamento y Compañía**: Departamentos pueden ser asignados a empleados, y Compañías a visitantes
- **Visitantes**: Cambio total en la pantalla + Posibilidad de imprimir tarjeta para un visitante
- **Informes: Personal Activo para TimeLOG** – Permite exportación de datos del empleado al TimeLOG
- **FPU**: Imágenes pueden ser guardadas en formato JPG, impresiones pueden ser guardadas en una tarjeta Mifare (validez a través de la tarjeta)
- **Opciones**: Respaldo para la lectora FPU-S USB.

1.4 Ediciones de Falcon

A seguir usted encontrará una lista de las diversas ediciones del *Falcon*. En la tabla especificada están las características que diferencian estas ediciones una de la otra:

	Característica	**Demo**	**Express**	**Five**	**Standard**	**PRO**
Terminales	Master + Acceso	+			+	+
	SY-400/SY-400A	+	+	+	+	+
	COM-II-PRO	+			+	+
	Controlador de Alarma ProSYS 128 de Rokonet	+				+
	Máximo de terminales definidos	1	1	5	255	255
Notificación de evento	SMS					+
	Ver/Editar mapa del sitio				+	+
	Localiza Ajuste de terminales Master a cambios de ahorro de luz diurna	+			+	+
Auto Modos	Definir auto modos del Master	+			+	+
Zonas Horarias	Definir zonas horarias del Master	+			+	+
Huellas Digitales	Máximo de plantillas por persona	1	2	2	10	10
Producción de Tarjeta	Editar croquis de la tarjeta	+				+
	Múltiples croquis	+				+
	Croquis Horizontal/Vertical	+				+
	Impresión Doble (cuando respaldado por la impresora)	+				+
	Captura imágenes vía el dispositivo TWAIN	+				+
	Captura firma de una almohadilla para firmas respaldada por Wintab					Especial
Varios	Máximo de tarjetas en la lista de Personal	5	Ilimitado	Ilimitado	Ilimitado	Ilimitado
	Módulo del Visitante	+		+	+	+
	Máximo de visitantes en lista	5	Ilimitado	Ilimitado	Ilimitado	Ilimitado
	Ejecuta un programa cuando el dispositivo de I/O es activado					+
	Impresión/Vista Previa/Exportación de informes		+	+	+	+
	Usuarios múltiples				+	+
	Importación manual de datos del personal				+	+
Programación automática	Importación automática de datos del personal			+	+	+
	Opciones en la línea de comando				+	+
En línea	Colección de datos en línea desde su controlador de alarma local ProSYS 128					+
	Muestra video al vivo cuando la tarjeta es fichada					+

Capítulo 2 – Instalación

Para instalar Falcon bajo: Windows NT, 2000, XP o 2003,
usted necesita privilegios de administrador.

Introducir el CD en la unidad, esperar algunos segundos por la operación automática del menú de instalación. Si el programa no empezar automáticamente, ir al archivo FalInst.exe y hacer doble clic, aparece la pantalla abajo:

A partir de la versión 2.20 del *Falcon*, el programa requiere un enchufe de protección al hardware. La tecla HASP es un dispositivo de hardware que se conecta al ordenador y forma parte de la seguridad del *Falcon*. La tecla HASP protege al usuario contra uso no autorizado del sistema y guarda piratería. La tecla HASP debe ser instalada o el software no podrá ser ejecutado.

Hay dos tipos de teclas HASP, aquellas que se conectan en el puerto USB y las que se conectan en el puerto paralelo.

2.1 HASP – Enchufe de Protección

La instalación puede ser:

1. Local, por estación de trabajo (enchufe por PC) – requiere la instalación de la unidad HASP (véase pantalla **FalInst**).
2. Un HASP en el servidor – requiere la instalación del License Manager del HASP en el servidor (véase la pantalla **FalInst**).

Nota: *La instalación puede ser evitada si el enchufe del HASP ya ha sido instalado.*
Si es una instalación de puerto USB usted debe primero instalar la unidad y solamente entonces insertar el enchufe.

Hacer clic o en el **HASP License Manager** o en el botón **HASP driver**. Seguir las instrucciones del asistente.
¡Después del HASP haber sido instalado con éxito, usted puede instalar el *software del Falcon*!

Nota: ¡Para compartir el **HASP** usando el **License Manager**, el puerto 475 del TCP debe estar abierto en el servidor y en sus clientes!

2.2 Software

Paso 1. Hacer clic en el botón **Install Falcon**. Usted debe desplazarse por el procedimiento de configuración.
Paso 2. El programa automáticamente ejecuta la configuración. Si durante la configuración se le requiere proveer información, hágalo como corresponde.

2.3 Instalación para Usuarios Múltiples

Instale como sigue:

Paso 1. Instale *Falcon* en cada PC en el sistema.

Nota: *Siga estrictamente estas directivas*:

1. *Abra Control Panel | BDE Administrator y en Configuration | System | Init determine Local Share como True.*
2. *Abra Control Panel | BDE Administrator y en Databases | Falcon determine PATH para ser una base de datos compartida.*
   Todos los clientes deben usar la misma EXACTA ruta al alias del Falcon (la misma unidad o el mismo nombre UNC y el mismo caso – mayúsculas o minúsculas – para todos los clientes).
3. *Falcon.exe debe ser ejecutado de una unidad local, cada cliente debe ejecutar su propia copia. No se recomienda la asignación de unidades (pueden ser accidentalmente eliminadas)! Use un nombre UNC (Universal Naming Connection): \\serverNAME\shareNAME\DB.*

Paso 2. Conecte un PC directamente a los terminales, este será la estación principal.

Paso 3. Defina todos los parámetros que crean una base de datos central común.

Paso 4. Copie esta base de datos y el archivo de fotos al servidor (cada un bajo un directorio designado).

Paso 5. Para crear una ruta de acceso al archivo de fotos, haga clic en **Setup [**Programa de Instalación**]** en el menú descendente y elija la carpeta **General Parameters [**Parámetros Generales**].** En la sección **Files and Directories [**Archivos y Directorios**]** haga clic en el botón a la derecha del campo **Photos [**Fotografías**]**.

Paso 6. Cada PC debe crear ahora una ruta de acceso a estos archivos en el servidor. En el menú principal haga clic en **Maintenance| Restore| Alias to restore**.

Nota: *Todas las estaciones del Falcon deben compartir un servidor bajo un nombre idéntico*.

Paso 7. Seleccione el directorio apropiado, haga clic en **OK**, confirme la nueva ruta de acceso. El programa **Reiniciará**.

Paso 8. Para una actualización de la configuración, salga y torne a entrar en el programa *Falcon*.

Paso 9. Repita los pasos 5–9 para ejecutar la configuración de cada PC en el sistema.

Nota: *Usted no puede ejecutar Falcon dos veces en el mismo PC.*

2.4 Opciones de la línea de comandos del *Falcon*

Falcon puede ser operado en el modo de proceso por lotes para ejecutar diversas actividades y después cerrarse.

El sintaxis es: **Falcon [/ai][/ac][/au][/av][/at**]. Los parámetros disponibles son:

/ai = Importación automática del archivo actual de datos del personal (un nombre de archivo puede ser determinado bajo el área **Automatic import [**Importación automática**]** en el campo **Import file name [**Nombre del Archivo de Importación**]**.

/ac = Colecta datos – Colecta transacciones de todos los terminales activos.

/au = Actualiza terminales – Envía las recientes actualizaciones (cambios desde la última actualización) a todos los terminales Master activos.

/av = Envía todas las tarjetas permitidas a todos los terminales activos.

/at = Envía la hora y fecha del PC a todos los terminales activos.

El Programador de Tareas del Windows puede ser usado para ejecutar automáticamente el *Falcon* en horarios designados.

Para configurar el programador de tareas en el Windows 98, 2000:

Paso 1. Vaya a **My computer | Scheduled tasks | Add scheduled task**.

Paso 2. Usando la barra de desplazamiento encuentre el software del *Falcon* y señálelo.

Paso 3. Haga clic en **Next**. (Usted puede dar un nombre a la tarea en lugar del nombre predeterminado). Determine la frecuencia, haga clic en **Next**.

Paso 4. Determine el **Start time [**Hora de inicio**]**, la frecuencia y el **Start date [**Fecha de inicio**]** y haga clic en **Next**.

Paso 5. Anote una contraseña de usuario (cualificado) en el campo **Enter the password [**Entre la contraseña**]**.

Paso 6. Marque la casilla de verificación **Open advanced properties for this task when I click finish [**Abrir propiedades avanzadas para esta tarea al hacer clic en Finish**]**. Haga clic en **Finish**. La pantalla de la tarea aparecerá. Agregue una barra diagonal "/" y los relevantes parámetros de la línea de comandos.

Nota: *Cuando usted ejecuta el Falcon con el comando AT el es ejecutado como un servicio, NO unidades mapeadas! Así, si usted establecer su alias en G:\db funcionará en el modo interactivo pero fallará al ser ejecutado del AT porque no puede encontrar la unidad G. Por este motivo, usted DEBE usar nombres UNC para todos los alias de clientes (y servidor).*

Para configurar el programador de tareas en el Windows NT:

Paso 1. Abra el **Command prompt**.

Paso 2. Teclee lo siguiente:

AT hh:mm [/EVERY:date] x:\Path\Falcon.exe [/ai] [/ac] [/au] [/av]
[/at]. i.e.: Para colección de datos de los terminales a la 1AM de la mañana a cada Lunes teclee:
AT 01:00 /EVERY:M c:\Falcon\Falcon.exe/ac

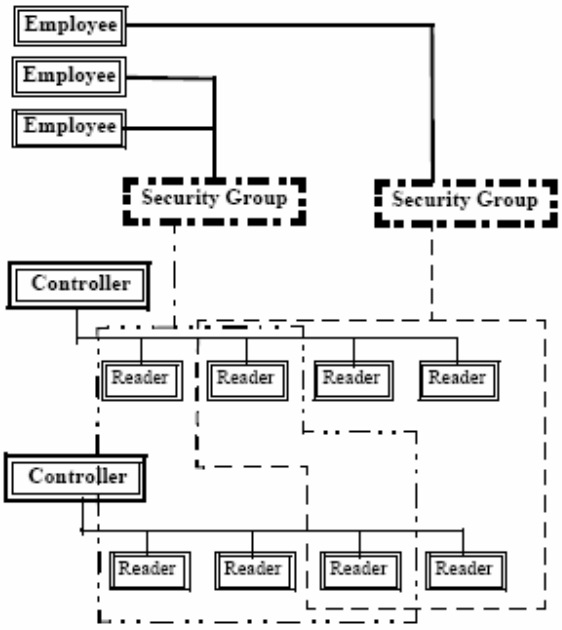
Nota: *Para NT, 2000, XP asegúrese que el servicio de programación de horario fue iniciado (consulte con el administrador del sistema para ayuda) y conéctese como usuario que tiene acceso autorizado a estos datos. Visto que el usuario predeterminado "System Account" no tiene acceso a los recursos de la red.*

Capítulo 3 – Configuración

3.1 Configurando el Sistema

Antes de iniciar la configuración se recomienda planear la estructura óptima del sistema: Esquematice la localización de la lectora según la cual los controladores serán colocados. La lista de empleados debe ser ordenada según una orden lógica: por departamento/función título/localización. Un planeamiento general de requisitos de tiempo y de localización para la generación del control de acceso debe ser delineado. Todavía, como etapa preliminar se recomienda permitir a todos los empleados acceso total, y después de un período de prueba iniciar la segunda etapa de ajustar los parámetros de control de acceso. Como los parámetros de autorización son dinámicos deben ser cambiados paulatinamente.

3.2 Croquis del Sistema



Iniciar la Configuración

Haga clic en el icono **Setup** en la barra de herramientas principal (Setup puede ser seleccionado alternativamente del menú). En el lado izquierdo de la pantalla aparece una lista de 11 carpetas. Estas son carpetas de ajuste que le ayudarán a configurar su sistema. Usted puede configurar su sistema en el orden delineado aquí.

Las carpetas son:

General Parameters **[**Parámetros Generales**]**	Security Group **[**Grupo de Seguridad**]**
Calendar **[**Calendario**]**	Events **[**Eventos**]**
Auto Modes **[**Modos Automáticos**]**	Communication **[**Comunicación**]**
Terminal list **[**Lista de Terminales**]**	**Report Generator [**Generador de Informes**]**
Time Zones **[**Zonas Horarias**]**	**Message Translation [**Traducción de Mensajes**]**

Los módulos resaltados son complementarios y opcionales.

3.3 Parámetros Generales

Estos le permiten definir la configuración global que afectará todas las estaciones del *Falcon*. Las definiciones para los Parámetros Generales están divididas en 4 categorías:

Configuraciones Predeterminadas
Configuraciones del Sistema
Configuraciones de Comunicación
Configuraciones de Archivos y Directorios

3.3.1 Configuraciones Predeterminadas

Se refiere a las configuraciones predeterminadas de su sistema *Falcon* que son utilizadas automáticamente al definirse un nuevo terminal. Cuando es necesario modificar los parámetros de un terminal o definir un nuevo terminal, las definiciones predeterminadas pueden ser reemplazadas según sus preferencias en la **Terminal List [**Lista de Terminales**]**.

Sección del Terminal:

Este grupo contiene campos que afectan las configuraciones predeterminadas para nuevos terminales.

Format **[**Formato**]** – Usted puede elegir uno de los formatos encontrados en el archivo PHANTOM.fmt.

Port **[**Puerto**]** – Define a que puerto de comunicación la unidad del controlador es conectada.

Baud Rate **[**Velocidad en Baudios**]** – Define la velocidad de comunicación en baudios.

Duress Code **[**Código de Amenaza**]** – Un código usado por un usuario amenazado por un intruso. Después de teclear este código se abre la puerta y un evento es enviado simultáneamente al ordenador host. Utilizado por la lectora de Acceso en el modo Tarjeta+PIN.

Maximum Cards **[**Máximo de Tarjetas**]** – La cantidad total de tarjetas usadas en un terminal master.

Global Anti-Pass-Back **[**Contra Nueva Fichada Global**]**- permite la prevención de más de una entrada por la misma puerta (para todas las lectoras conectadas al mismo controlador) hasta que la misma tarjeta sea utilizada en uno de los otros terminales definidos en la tabla **Terminal Dependencies**.

Sección de la Tarjeta:

Consiste en la localización y la definición de la longitud de la cadena de dígitos a ser leídos por los terminales esclavos; incluye también la fecha de vencimiento.

Start **[**Inicio**]** – La localización del primer carácter a ser leído de la tarjeta. La parte de la cadena magnética que será leída e incluida en las definiciones predeterminadas.

Length **[**Extensión**]** – El número de caracteres en la cadena a ser leída.

Max. Length **[**Máxima Extensión**]** – El número total de caracteres en la cadena.

Expire Date **[**Fecha de Expiración**]** – La fecha de expiración predeterminada para nuevos empleados.

Set Group **[**Configurar Grupo**]** – Un grupo de seguridad predeterminado para todos titulares de tarjeta.

Set Visitor Group **[**Configurar Grupo de Visitantes**]** – Un grupo de seguridad predeterminado para todos los visitantes.

3.3.2 Configuraciones del Sistema

Los campos en este grupo definen las configuraciones que afectan el interfaz del *Falcon* con el PC y el mundo exterior.

Sección de localización

Language **[**Idioma**]** – El idioma seleccionado es usado para exhibir el texto en el PC. Elija también la dirección del interfaz del usuario.

Summer Time / Winter Time **[**Horario de Verano / Horario de Invierno**]** – Determina si y como los terminales serán ajustados para el modo Hora de Verano.

Sección del diseño de la tarjeta (solamente en la versión PRO)

Generate Picture Name from Index **[**Crear Nombre de la Imagen del Índice**]** – Para tarjetas de proximidad, permite crear el nombre de la imagen en el número de índice del empleado en vez de su número de tarjeta (hasta que usted imprime la tarjeta de proximidad usted no sabe su número).

Photo Ratio **[**Razón de la Foto**]** – La razón predeterminada para capturar la foto de las personas es 0.77; usted puede cambiarla a 0.75.

Nombre de la Empresa para informes

Si usted desea agregar el nombre de la empresa en la cabecera de sus informes, anote el nombre aquí.

Sección de huellas digitales

FPU Type **[**Tipo FPU**]** – Existen distintos métodos de validación de huellas digitales; elija uno para todas las lectoras según el tipo de terminal a su disposición. Para más información, véase Huellas Digitales, en la página 71.

Templates per Person **[**Plantillas por Persona**]** – Determinan cuantos dedos pueden ser apuntados para un empleado.

Show Template Image **[**Mostrar Imagen de la Plantilla**]** - Si mostrar la imagen de la plantilla después de la inscripción (pantalla del Empleado). Al ver la plantilla apuntada, el registrador puede determinar si la calidad de la plantilla es suficiente, o si una nueva inscripción debe ser realizada. También, si la inscripción es problemática, el origen puede ser seguido (dedo, unidad etc.)

Save Template Image **[**Guardar Imagen de la Plantilla**]** – Después de la inscripción, las imágenes de la plantilla pueden ser guardadas en formato JPG bajo el mismo directorio de las plantillas de las huellas digitales. Para cambiar la ruta véase el Capítulo 15 – Huellas Digitales, en la página 71.

Sección Exhibir estos Terminales

Es posible desactivar todos los tipos de terminales que no son usados en su sistema. Por predeterminación, el controlador Master y sus unidades de Acceso son exhibidos. Todos los parámetros relevantes serán desactivados consecuentemente.

3.3.3 Configuraciones de Comunicación

Sección de Comunicación

Retry **[**Reintentar**]** – Representa cuantas veces el programa de comunicación intenta ejecutar un comando en caso de un error.

Time Out **[**Tiempo de Espera**]** – El periodo de tiempo (en segundos) que el host espera por una contestación del controlador.

Time between Blocks **[**Tiempo entre Bloques**]** – Tiempo de espera (en milisegundos) entre bloques consecutivos mientras se comunican con un terminal.

Remote update **[**Actualización remota**]** – Permite actualizar datos del Personal a terminales desde estaciones de trabajo remotas. Al compartir su DB con más de una estación de trabajo, solamente una estación puede comunicarse con los terminales. Nuevos datos son acumulados, y durante una actualización, la estación de trabajo que se comunica los repasa y envía los datos relevantes (implementados diferentemente para cada tipo de terminal) al terminal. En su estación de trabajo usted debe: Ir a **Tools | Options | Automatic Scheduling | Frequency**, sob **Update Terminals [**Actualizar Terminales**]** y establecer un valor de frecuencia superior a 0.

Seleccione el tipo de terminal que será actualizado. Para cada tipo de terminal las actualizaciones serán realizadas de manera distinta:

- **None [**Ninguna**]** – Ninguna actualización será enviada automáticamente. Las actualizaciones pueden ser enviadas (cuando requerido) manualmente a través de la pantalla **Communication [**Comunicación**]** o vía **Personnel | Send Last**. Esta opción es relevante cuando se trabaja con un PC solamente que está conectado a un terminal Master, o si no hay necesidad para actualizaciones recurrentes.
- **Master** – El PC enviará todas las actualizaciones desde la última actualización.
- **SY-400** – El PC enviará todas las actualizaciones acumuladas desde la última completa programación.
- **COM-II-PRO** – El PC reenviará la lista completa autorizada a todos los terminales COM-II-PRO.

Save Comm Errors in DB **[**Guardar Errores de Com. en la DB**]** – Señale esta casilla de verificación para guardar en línea en la DB errores de comunicación con el controlador, mientras creando un evento correspondiente.

Write Last Transaction into Personnel File **[**Escribir la Ultima Transacción en el Archivo Personal**]** – Escribe la última transacción del empleado en el registro del empleado. Reduce el contador para el tipo de empleado **Active – countdown**. Cuando el contador llega a cero el programa cambia el tipo de empleado para **Countdown reached 0**. Esta información puede ser encontrada bajo: **Personnel | Employee details | Management**. Esta información será usada más tarde en el informe **Absence**.

Este procedimiento no actualiza el terminal. Así:

- Los terminales Master tienen un contador y requieren este procedimiento para actualizar el PC.
- Los terminales SY-400 pueden:
  Usar el SYServer para conteo en línea O
  El conteo del PC será actualizado en el terminal enviándole regularmente la lista autorizada.

Nota: *Como este procedimiento requiere una búsqueda del empleado puede retrasar la colección de datos!*

Send Visitor Cards to Terminal **[**Enviar Tarjetas de Visitantes al Terminal**]** – Si esta casilla de verificación está señalada (predeterminado), entonces durante la emisión/devolución de las tarjetas de visitantes el estatus de la tarjeta en la lista de Personal cambiará como consecuencia y será enviado a todos los terminales activos (inmediatamente al terminal Master y durante las actualizaciones a los terminales SY-400).

Nota: *Para los terminales SY-400, se recomienda desactivar esta casilla, y de esa manera mantener todas las tarjetas disponibles todo el tiempo!*

Enforce Induction Date **[**Implementar la Fecha de Inducción**]** – El tiempo medido desde la última fecha de re-certificación periódica de seguridad. Pasado este tiempo el empleado será bloqueado hasta ser re-certificado.

Sección Parámetros del Master

Door Button Group **[**Grupo Botón de Puerta**]** - En terminales Master, asignar un grupo de seguridad a un terminal permite la operación de su botón de puerta para el tiempo predefinido para ese grupo.

Nota: *Dos eventos son dedicados para indicar el uso de botones de puerta:*
- Puerta abierta por botón
- Botón de puerta no autorizado

Sección Parámetros del SY-400

Technician card **[**Tarjeta del técnico**]** – El número definido será usado como el número de tarjeta del técnico para todos los terminales SY-400.

3.3.4 Configuraciones de Archivos y Directorios

Esta carpeta contiene la ruta para cada uno de los siguientes archivos:

Phantom Path **[**Ruta del Phantom**]** – Ubicación del programa de comunicación del sistema (Phant32.exe)

Data **[**Datos**]** – Ubicación de la Transacción.

Backup **[**Copia de Seguridad**]** – Ubicación del archivo de la copia de seguridad de Transacciones.

Project Directory **[**Directorio del Proyecto**]** – Se refiere a la ubicación del directorio **Tables [**Tablas**]**.

Photos Directory **[**Directorio de Fotografías**]** – Ubicación de las fotografías.

Signatures Directory **[**Directorio de Firmas**]** – Ubicación de las copias de firmas (solo en la versión PRO).

3.4 Herramientas

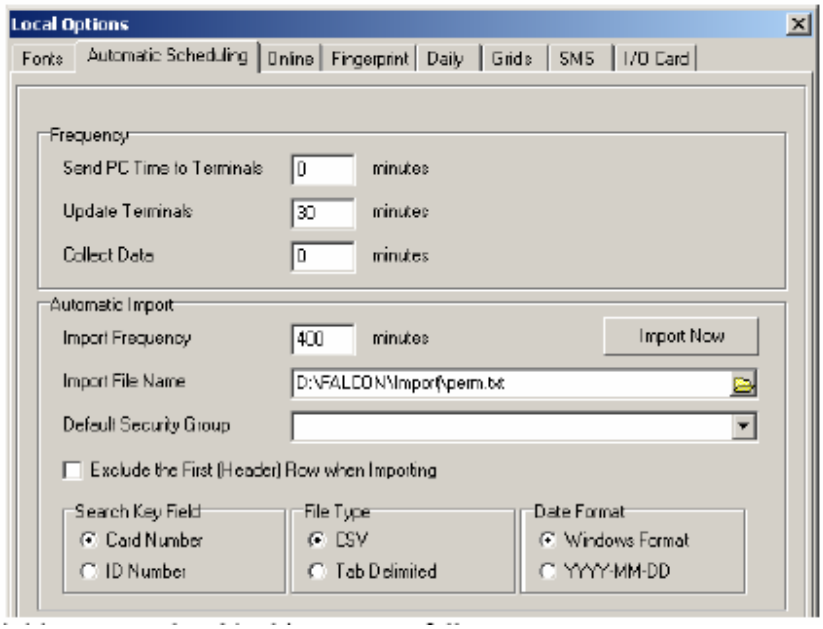
3.4.1 Opciones

Esta característica permite ajustar la configuración y parámetros de su estación de trabajo **local** (no afecta a otras estaciones de trabajo!).

3.4.1.1 Fonts [Fuentes]

Permite definir el tipo y tamaño de la fuente del interfaz (Barra de Herramientas, barra de configuración, barra de estatus).

3.4.1.2 Automatic scheduling [Programación automática]



Todas las actividades automáticas son reguladas en esta pantalla como sigue:

Sección Frequency [Frecuencia]

- Envía la fecha y hora del PC a los terminales.
- Update Terminals **[**Actualizar Terminales**]** – Envía las recientes actualizaciones (cambios desde la última actualización que incluyen también nuevas plantillas de huellas digitales) a todos los terminales activos del tipo seleccionado en **Setup | General Parameters |Communication | Remote Update.**
- Collect Data **[**Colectar Dados**]** – Colecta transacciones de todos los terminales activos.

Sección Automatic import [Importación automática]

Importación automática del actual archivo de datos del personal (un nombre de archivo puede ser determinado en el **Automatic import [**Importación automática**]** en el campo **Import file name [**Nombre del archivo de importación**]**. Este archivo es creado por otro programa. El *Falcon* recupera los datos relevantes y elimina el archivo de actualización. Los datos de cada persona aparecen en una línea separada, con comas/tabulaciones entre los campos y cada línea termina con CR+LF.

Los campos son:
Card-number, Name, Type, Group-1, Date-1, Time-1, Description, Department, Position, Employee-number, Photo, Pop-type, Phone, Cell-Phone, PIN, PIN-Required, Group-2, Group-3, Group-4, Group-5, Date-2, Date-3, Date-4, Date-5, Time-2, Time-3, Time-4, Time-5, First-name, Middle-name, Family-name, City, Street, House-Number, Apartment, Zip-Code, District, Birthday, Induction-Date, Signature, Expected- Swipes.

A seguir una explicación elaborada con respecto a los campos principales:

Tipo:

-3	Robado
-2	La cuenta regresiva llego a 0
-1	Suspendido
0	Bloqueado (no activo, es imposible borrar tarjetas por importación)
1	Activo
2	Cuenta regresiva activa
3	Activo deshabilitado

Group (1-5) [Grupo**]**: Nombre o ID del grupo de seguridad (si usted anota 0, usted borra el grupo de seguridad actual. Deje este campo vacío para obtener el grupo de seguridad predeterminado):

Nota: *La ID del grupo puede ser vista en el informe **Readers per Group [**Lectoras por Grupo**]** o en la pantalla **Edit Security Group [**Editar Grupo de Seguridad**]** (lado izquierdo inferior).*

Date (1-5) [Fecha**]:** Las fechas opcionales de caducidad (por grupo de seguridad), deben ser en:

- Un formato Windows como definido en: **Control panel | Regional settings | Date | Short date format**.
- Un formato fijo: YYYY-MM-DD

Time (1-5) [Hora**]:** El horario opcional de caducidad (por grupo de seguridad), debe ser en el formato HH:mm.

Description [Descripción**]**: Cualquier información relevante que pertenece a la tarjeta.

Population type [Tipo de población**]**: 0 - Regular, 1 - Visitante, 2 - Guardia

PIN: código personal de cuatro dígitos

PIN Required [PIN Requerido**]:**

0 – la casilla de verificación en la pantalla **Employee details [**Detalles del empleado**]** no será activada.

1 – la casilla de verificación en la pantalla **Employee details** será activada.

Todos los campos excepto el número de tarjeta son opcionales. Asegúrese que todos los campos irrelevantes estén vacíos y el sistema no los tomará en cuenta (El sistema no toma en cuenta espacios iniciales y finales).

Campos que contienen comas (por ejemplo: **Description**) deben utilizar comillas de modo que el software trate el texto dentro de las comillas como un campo, es decir: 123456, "Kedem, Chen", 1; para saltar un campo sin actualización deje su espacio vacío: 123456, 1 para borrar el contenido del campo: 123456, " ", 1 (observe el espacio entre las comillas).

Default Security Group **[**Grupo de Seguridad Predeterminado**]**:

Como parte del proceso de importación se puede definir un grupo de seguridad predeterminado para todos los archivos de empleados importados recientemente en el campo **Default Security Group [**Grupo de Seguridad Predeterminado**]**como sigue:

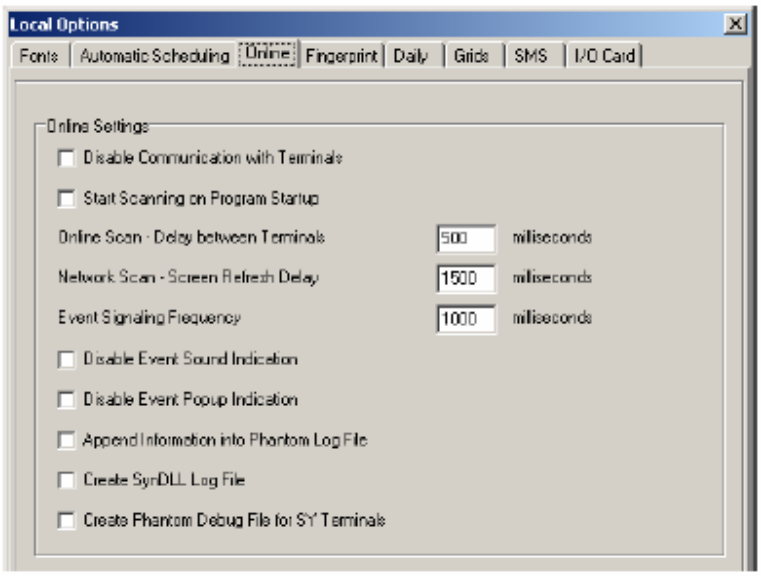
- Si es un nuevo empleado el programa insertará el número del grupo de seguridad predeterminado.
- Si es un empleado existente el número del grupo de seguridad no cambiará.

Exclude the First (Header) Row when Importing **[**Excluir la Primera Fila (Cabecera) al Importar**]** – Al importar archivos Excel CSV se puede excluir la cabecera que es generalmente la fila del título de su archivo de destino.

Search Key Field **[**Campo Llave de Búsqueda**]** - Emparejar la base de datos actual y la base de datos importada es hecho según llaves del número de tarjeta o del número de ID. Para el número de tarjeta el software verifica que cada número sea único. ¡Todavía, para el número de ID es responsabilidad del operador cerciorarse de que las ID sean únicas!
File Type **[**Tipo de Archivo**]** - Usted puede importar un archivo de origen o en formato delimitado por coma (CSV) o en formato delimitado por tabulación.
Date Format **[**Formato de la Fecha**]** - Usted puede importar el archivo de origen en un formato de fecha de Windows o en un formato fijo: YYYY-MM-DD.

3.4.1.3 Online [En línea]

Permite definir configuraciones en línea, como sigue:



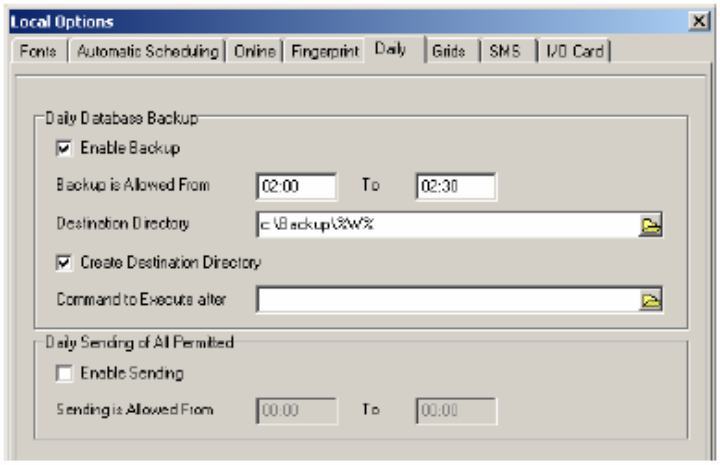
Disable Communication with Terminals **[**Desactivar la comunicación con los terminales**]** – Todas la actividades de comunicación pueden ser desactivadas por estación de trabajo.
Start scanning on Program Startup **[**Empezar a examinar en el Inicio del Programa**]** – Activando esta casilla de verificación inicia la consulta del terminal. El examen es activado cuando el software comienza.
Online Scan Delay between Terminals **[**Retraso de la exploración en línea entre Terminales**]** – El tiempo pasado entre los terminales durante la exploración en línea. El retraso posibilita tiempo de CPU disponible para otras tareas. Si usted anota un valor inferior a 300 esto puede sobrecargar su PC.
Network scan - Screen Refresh Delay **[**Exploración de la red – Retraso en Actualizar la Pantalla**]** – El retraso entre cada actualización.
Event signalling frequency **[**Frecuencia de señalización de evento**]** – La frecuencia para señalización de evento en otras estaciones de trabajo. Usado generalmente apenas para las estaciones de trabajo, no para el PC que recoge los datos (porque este PC inicia el envío de estos eventos) para activar mensajes emergentes y sonidos de notificación.
0 = sin operación – para usuario individual o para operadores que no requieren notificación de evento.
Disable Event Sound Indication **[**Desactivar la Indicación de Sonido de Evento**]** – Desactiva cualquier indicación de sonido de evento.
Disable Event Popup Indication **[**Desactivar la Indicación Emergente de Evento**]** Desactiva cualquier indicación emergente de evento.
Los ítems siguientes son dedicados a trazar cualquier problema que pueda ocurrir en su software:

Append Information into Phantom Log File **[**Anexar Información en el Archivo de Registro Phantom**]** – Permite guardar indefinidamente Registros Phantom (si esta casilla de verificación está desactivada, el phantom.log será limpiado y reescrito para cada actividad Phantom.
Create SynDLL Log File **[**Crear el Archivo de Registro SynDLL**]** - El syndll.log registra datos en línea. Los datos acumulados pueden ser de gran volumen, por lo tanto se recomienda usarlo solamente para rastrear problemas.
Create Phantom Debug File for SY Terminals **[**Crear el Archivo de Depuración Phantom para los Terminales SY**]** – El synelcom.log documenta todas las actividades de la comunicación de nivel bajo del SY-400. Es limpiado siempre que se activa el Phantom.

3.4.1.4 Fingerprint [Huellas Digitales]

Véase Capítulo 15 – Huellas Digitales, en la página 71.

3.4.1.5 Daily [Diariamente]



Sección Daily Database Backup [Copia de Seguridad Diaria de la Base de Datos**]**
Posibilidad de copiar, una vez al día, todas las bases de datos a otro directorio para propósitos de copia de seguridad. El sistema señala todas las estaciones de trabajo para cerrar sus bases de datos temporalmente para asegurar una copia de reserva exitosa.
El directorio de la copia de seguridad puede ser fijo, y será eliminado durante la copia de reserva. Es también posible anotar una variable en el campo **Destination Directory [**Directorio de Destino**]** como sigue:

%YYYY%	Año actual en un formato de cuatro dígitos.
%YY%	Año actual en un formato de dos dígitos.
%MM%	Mes actual en un formato de dos dígitos.
%DD%	Día actual en un formato de dos dígitos.
%W%	Día de la semana donde: 1= Domingo, 2= Lunes etc.

Create Destination Directory **[**Crear Directorio de Destino**]** - Si no existe directorio de destino, él será creado. Si la casilla de verificación no está señalada, asegúrese de que existe un directorio de destino antes que la copia de seguridad inicie.
Así, cada vez que un nuevo nombre de archivo sea creado, el archivo viejo no será suprimido. Después de concluida la copia de seguridad es posible ejecutar un programa externo (Por ejemplo: para transferir/suprimir archivo, etc.).
Sección Daily Sending of All Permitted [Envío Diario de Todo Autorizado**]**
Envía todos los detalles de empleados autorizados a todos los terminales activos, una vez al día.

3.4.1.6 Grids [Cuadrículas]

Posibilita guardar / no guardar las preferencias de cuadrícula del usuario:

Use default settings **[**Usar la configuración predeterminada**]** - El software usa el conjunto predeterminado en el archivo exe del programa.
Load user settings from disk **[**Cargar configuración del usuario desde el disco**]** - el software usa los cambios realizados por el supervisor (en **Load user settings from disk. Save settings on exit**), pero no guarda ningún cambio adicional.
Load user settings from disk, save settings on exit **[**Cargar configuración del usuario desde el disco, guardar la configuración al salir**]** – los cambios realizados por el usuario serán guardados todas las veces al salir.

3.4.1.7 SMS (solamente en la versión PRO)

El Short Message Service (SMS) es similar a un buscador de personas (paging). Es un servicio para enviar cortos mensajes de texto a teléfonos móviles. Actualmente el *Falcon* usa:

1. Modem Ericsson DM-10/DM-20 SMS.
2. Dispositivos GSM.

Primeramente, usted debe definir todos los parámetros de comunicación SMS en **Tools| Options| SMS** como sigue:

Port **[**Puerto**]**
Baud rate **[**Velocidad en baudios**]** - generalmente 9600
Time out (between transmissions) **[**Tiempo de espera (entre transmisiones)**]** – debe exceder a 2-3 segundos – tiempo para transmisión del mensaje + contestación para el SMSC.
SMS modem **[**Modem SMS**]** – elija un modem compatible.
Message encoding **[**Codificación del mensaje**]** – configurar la codificación del remitente. Si no coincide con la codificación del receptor el mensaje no será recibido o será recibido confusamente:

- IRA (International Reference Alphabet) – alfabeto de la lengua inglesa
- ISO 8859-1 - Latin 1 – cubre la mayoría de los idiomas europeos occidentales
- ISO 8859-8 - LATIN/Hebrew – usado para Hebreo e Yiddish
- Unicode – proporciona un número único para cada carácter, no importa qué plataforma o lengua.

Ahora, usted debe conectar el modem en el puerto definido del PC (puerto RS-232).
En *Falcon*, los mensajes SMS son enviados durante un evento. Para enviar un mensaje usted debe hacer lo siguiente:

Paso 1. Vaya a **Event | General**, la descripción del evento será el contenido del mensaje SMS correspondiente.

Paso 2. Defina el evento y anote el contenido del mensaje. El mensaje incluirá también: fecha, hora, número de tarjeta y el terminal implicado en este evento.

Paso 3. Sob **Event | Automatic Activity** usted puede elegir a qué suscriptor será enviado el mensaje de SMS (Después de usted haber manualmente anotado todos los números de teléfono móvil relevantes del suscriptor - un número por fila! Usted puede utilizar el punto y coma para observaciones del remitente como texto a la derecha del; el símbolo no será visible).

El botón **Test** es usado para enviar un mensaje de prueba. El suscriptor(es) designados deben verificar si fue recibido completa y correctamente.

3.4.1.8 I/O Card **[**Tarjeta I/O**] (solamente en la versión PRO)**

Falcon utiliza un puerto serial estándar RS-232 o una tarjeta de adquisición de datos dedicada a probar una señal de entrada. Cuando la señal cambia, realiza un programa externo y/o abre todas las puertas de emergencia. Por ejemplo, cuando un circuito del sistema de alarma de incendio se cierra *Falcon* abrirá todas las puertas y ejecutará un programa de informe de fuego.
Dos tipos distintos de tarjeta son respaldados por *Falcon*:

- Prueba del puerto serial RS-232 de una señal de entrada CTS
  Para operación use los pernos 5, 8 en un conectador DB9 o 5, 7 en un DB25, a ser accionado con 3-12Vdc.

- Tarjeta digital de adquisición de datos PCI-7250 de ADLINK para pruebas de entradas digitales. Si usted trabaja bajo Windows 95', elija solamente Win 95, de lo contrario elija la otra opción. (Para la instalación refiérase a las instrucciones de instalación del fabricante).

Establezca los parámetros del dispositivo operacional:

Paso 1. Elija el tipo de tarjeta relevante y su designado puerto.

Paso 2. Velocidad de prueba: frecuencia de prueba de la señal.

Paso 3. Estado Activo de la Entrada: Alto/Bajo son niveles eléctricos a ser probados. Alternar – cualquier alteración activará una reacción.

Paso 4. Haga clic en el botón examinar en el campo **Command Line to Execute [**Línea de Comando a Ejecutar**]** para insertar la ruta del programa a ser operado.

Paso 5. Si usted quiere que todas las puertas se abran durante una emergencia, marque la casilla de verificación **Open All Emergency Doors [**Abrir todas las Puertas de Emergencia**]**.

Nota: *Las características de la tarjeta SMS/Fingerprint/I/O son puerto RS-232 designadas*.

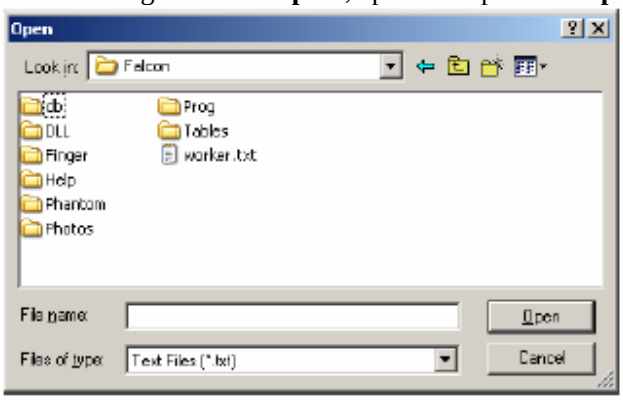
3.4.2 Importar Archivos del Personal

Falcon permite la importación de archivos de texto para registrar nuevos empleados manual o automáticamente (véase 3.4.1.2 Programación automática, en la página 12). Estos métodos de importación se diferencian en la estructura del archivo. También, en la importación automática, el archivo importado es borrado después de reprocesado.

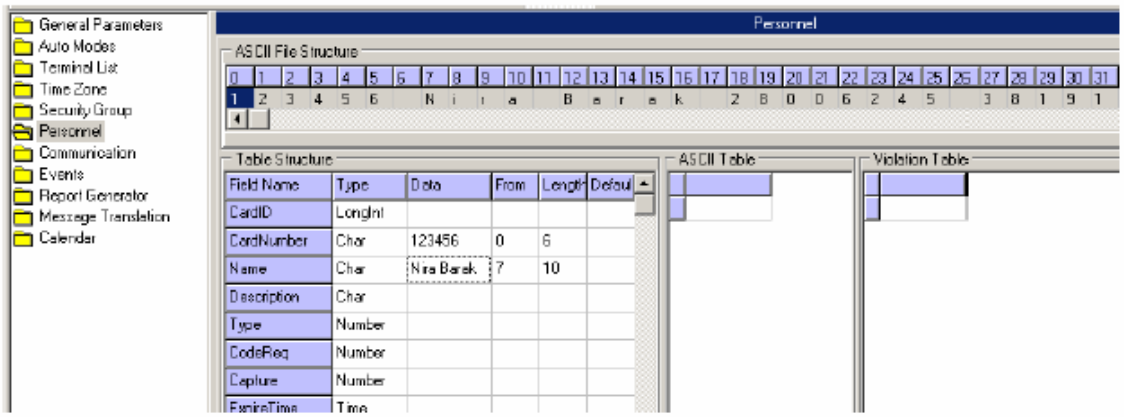
Los archivos de texto manualmente importados están basados en una plantilla definida por el usuario, donde cada línea en el archivo es el registro para una persona, cada campo está en una posición fija y CR+LF está en el final del vínculo. El procedimiento de importación es como sigue:

Paso 1. Haga clic en **Setup**, después haga clic en la carpeta **Personnel [**Personal].

Paso 2. En la pantalla **Personnel** haga clic en **Import**; aparece la pantalla **Open**.



Paso 3. Seleccione su archivo de **texto** Import (creado anteriormente); la pantalla **Import** aparece (abajo).



Nota: *Los detalles de la primera línea en el archivo de importación aparecen bajo el título* **ASCII File Structure.**

Paso 4. Para continuar con el proceso de importación, marque un ítem del dato, después haga doble clic en el espacio **Type** enfrente al título relevante.

Paso 5. Repita esto para todos los restantes ítems de datos.

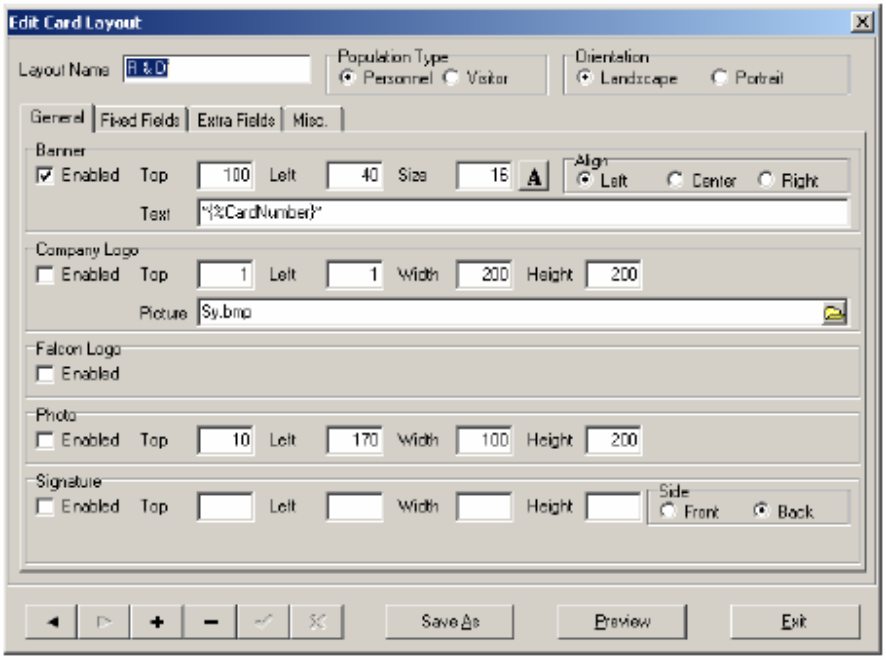
Paso 6. Para actualizar los siguientes detalles del empleado haga clic en el icono **Next**.

Paso 7. Para una presentación de los nuevos nombres haga clic en el botón **View ASCII**.

Paso 8. Haga clic en **Import** en la parte inferior de la pantalla; el archivo ASCII es ahora importado en la base de datos del programa. Haga clic en **Close** para salir de la función importación.

3.4.3 Editar Distribución de la Tarjeta (solamente en la versión PRO)

Usted puede editar la disposición de la tarjeta en **Tools | Edit Card Layout**, y a seguir en **Personnel | Employee details |Management | Card layout** asignar un diseño específico a un empleado.



Primero usted debe decidir si desea que la tarjeta sea impresa Landscape (horizontal) o Portrait (vertical). Después usted establece las dimensiones como corresponde.
Hay dos configuraciones distintas de tarjeta, **Personal** y **Visitante**. En la tabla siguiente están indicadas las diferencias entre los tipos de tarjetas:

Tarjeta de Personal	**Tarjeta de Visitante**
Fotografía	-------
Firma	-------
Departamento	Compañía
Número de ID	Nombre del Anfitrión
Grupo de Cálculo	Departamento Anfitrión
Autorización de la Policía	Acompañamiento Requerido

Hay cuatro fichas: General, Fixed fields, Extra fields y Misc. Use los siguientes botones para navegar y editar:

- Volver a la anterior Disposición de Tarjeta
- Pasar a la siguiente Disposición de Tarjeta

- Insertar una nueva Disposición de Tarjeta
- Eliminar la actual Disposición de Tarjeta
- Guardar las alteraciones
- Cancelar las alteraciones desde la última acción de guardar

General

Señale la relevante casilla de verificación y anote los campos Título*, logo de la Compañía, logo de Falcon, Fotografía y firmas.

* El título es donde usted puede escribir texto en la tarjeta. Aparte del texto sin formato que puede simplemente ser anotado, es posible también codificar tarjetas magnéticas o imprimir código de barras usando la impresora compatible, y utilizando los siguientes macros:

{Número}	Inserta el valor de un carácter ASCII como especificado en los paréntesis o sea {64}=@	
{% nombre del campo Empezar de, extensión}	nombre del campo	Anote el nombre del campo del archivo del empleado, o sea **Description**
	Empezar de	Mostrar la posición para el nombre del Campo definido (si quiere que solamente parte de los datos sea exhibida).
	extensión	Cuantos caracteres serán exhibidos a partir de punto de posición. Si ningún valor es anotado todo el campo será insertado.

Fixed fields [Campos fijos**]**

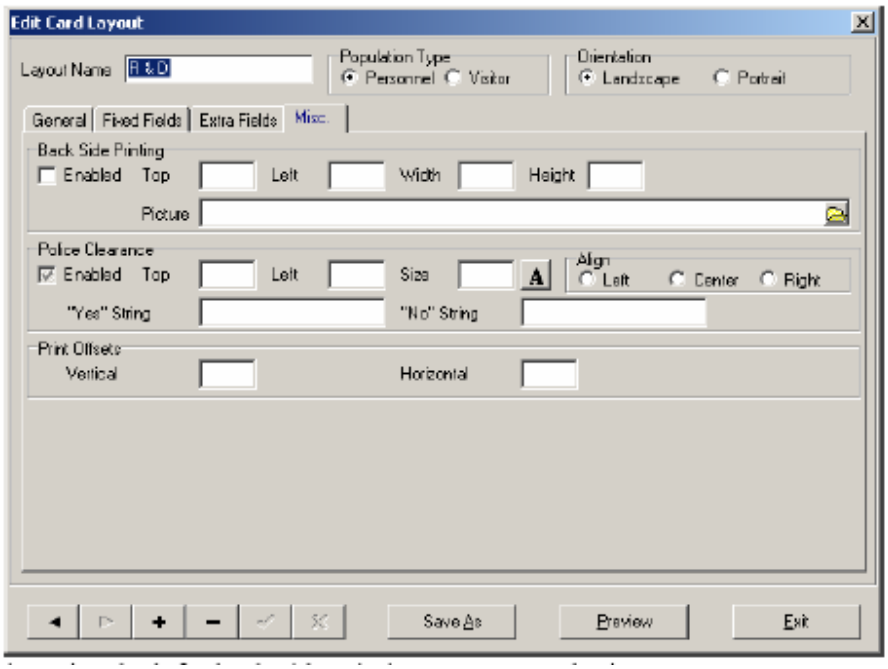
Señale la relevante casilla de verificación y anote el nombre de la Persona, el número de Tarjeta, el Departamento.

Extra fields [Campos extra**]**

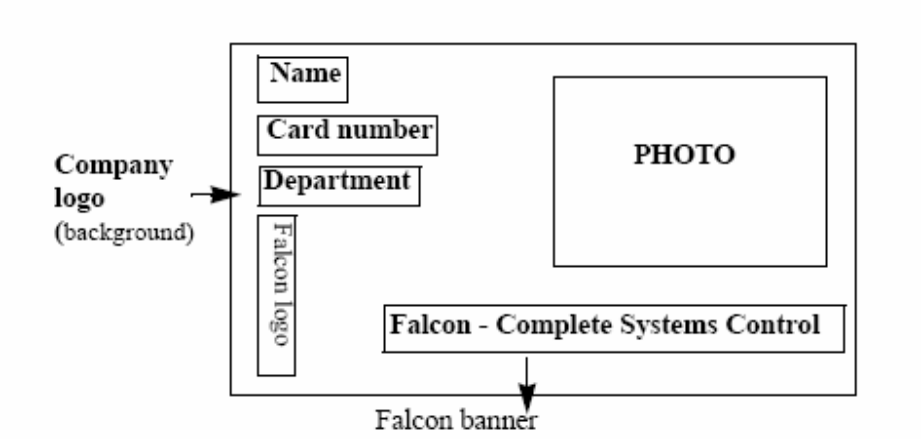
Señale la casilla de verificación relevante y anote los Campos Extra 1/2/3/4.

Nota: *Para imprimir la fecha actual usted debe seleccionar* **ISSUE_DATE** *del campo* **Field Name**.

Misc.



Usted puede utilizar esta ficha opcional para imprimir en el verso de la página en impresoras que respaldan esta característica.
En el campo **Picture**, elija una fotografía de fondo.
Note: *Las dimensiones son en píxeles.*
La plantilla será en orden alfabética incremental (según el nombre de la plantilla)



Police Clearance/Escort Required **[**Autorización de la Policía / Acompañamiento Requerido**]**

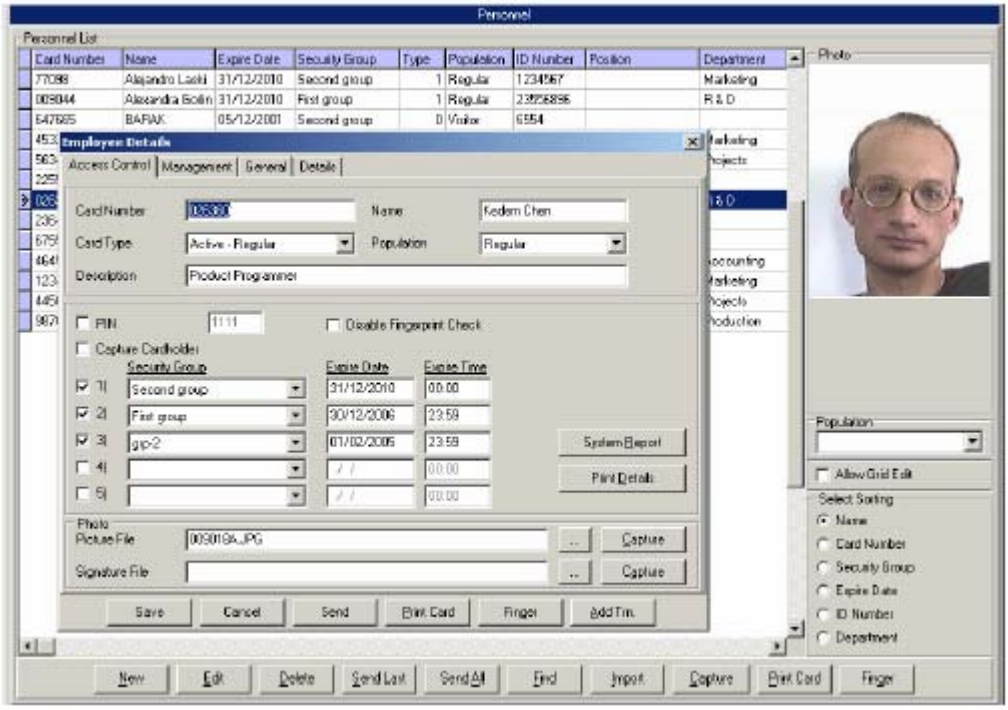
Hay dos campos: **Yes** y **No**. Si esta casilla de verificación está señalada: El contenido anotado en el campo **Yes** será impreso si la equivalente casilla de verificación bajo **Employee Details | Details** o bajo **Visitors** estuviera señalada (sob los campos: **Police Clearance** o **Escort Required**), y el contenido del campo **No** será impreso si estas casillas de verificación no estuvieran señaladas.

Print Offsets **[**Imprimir Posiciones**]**

Permite desplazar la disposición editada en su totalidad, en el marco de la tarjeta. El cambio será evidente solamente después de la impresión (no será reflejado en la pantalla **Edit Card Layout [**Editar el Croquis de la Tarjeta**]** o en la pantalla **Preview [**Vista Previa**]**).

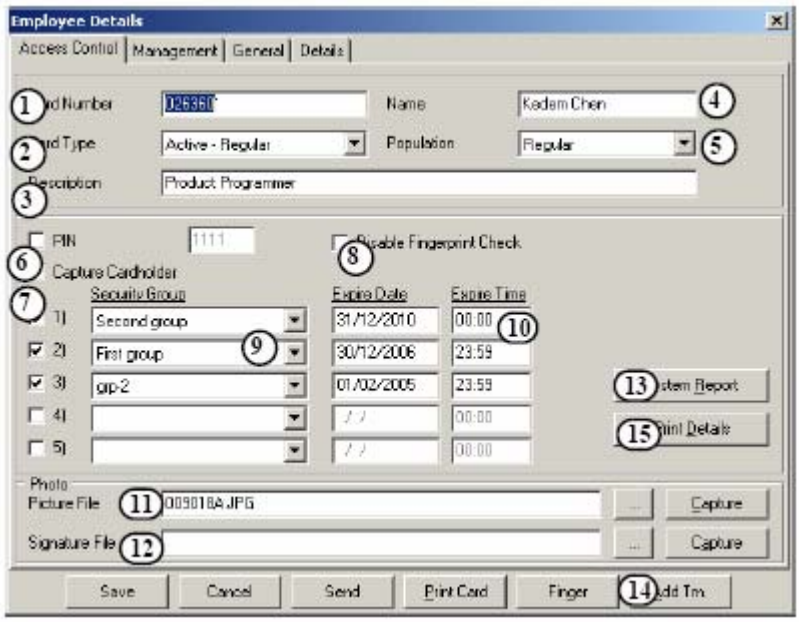
Capítulo 4 – Personal

Bajo Personal usted puede abrir archivos de Empleados que incluyen toda la información al respecto del empleado específico, de la organización y también información personal. Véase la pantalla abajo:



En el lado derecho de la pantalla usted puede ordenar los empleados por su tipo de población: Regular, Visitante o Guardia o no ordenar del todo. Véase la lista en el lado derecho para ordenar los datos del empleado.

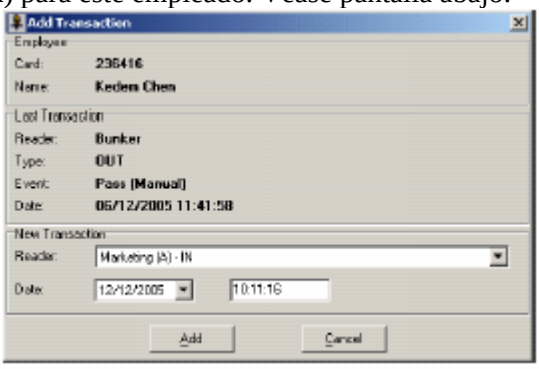
4.1 Definir parámetros para un nuevo empleado



La pantalla **Employee details [**Detalles del Empleado**]**en la carpeta **Personnel [**Personal**]** permite abrir un archivo nuevo de empleado, como sigue:

4.1.1 Ficha de control de acceso

Ref.	Nombre del campo	Descripción
1	Card number **[**Número de tarjeta**]**	Número codificado de la tarjeta del Empleado.
2	Card type **[**Tipo de tarjeta**]**	Atribuir un tipo de tarjeta (inducido por el terminal) a un empleado: Robada – Una tarjeta inactiva que puede ser considerada como robada cuando trabajando con el Servidor SY. Al señalar la casilla de verificación **Capture [**Captura**]**, la entrada será permitida al empleado y el/ella pueden ser "capturados"! Cuenta regresiva llegó a 0 – La tarjeta es bloqueada después que el contador de entrada llegó a 0. Suspendida – Bloqueo temporario por el operador o el sistema. Bloqueada – Un bloqueo permanente por el operador. Activa –Regular – Trabajando en una organización en base regular Activa – Cuenta regresiva – Trabajando temporalmente y con permisión para entrar/salir un número de veces predeterminado (solamente Master) Para información complementar (SY-400) véase párrafo 3.3.2 Configuración del Sistema, en la página 10. Activa – Permitida sin conexión – este tipo de tarjeta será enviado a las unidades de acceso para ser almacenado cuando no hay comunicación con el Master.
3	Description **[**Descripción**]**	Texto libre
4	Name **[**Nombre**]**	Nombre y apellido del titular de la tarjeta
5	Population **[**Población**]**	Refiérase a los derivados del control de acceso de la posición del titular de la tarjeta
6	Pin/count	Según el tipo de tarjeta: Regular – código-pin – un código adicional clasificado introducido e Cuenta – Cuenta – Limitación de acceso designada
7	Capture Cardholder **[**Capturar Titular de la Tarjeta**]**	Permite a un titular de tarjeta accionar un evento en el relé lógico (relé 2) (solamente Master)
8	Disable Fingerprint check **[**Deshabilitar Chequeo de Huellas Digitales**]**	Cuando esta casilla de verificación está señalada el empleado puede entrar en las premisas sin el requisito de huellas digitales.
9	Security group **[**Grupo de Seguridad**]**	Un empleado puede ser asignado a hasta 5 grupos de seguridad. Para más información véase el párrafo 5.5 Definir un Grupo de Seguridad, en la página 43.
10	Expire date/time **[**Fecha/hora de prescripción**]**	Después de esta fecha la tarjeta no será más válida para el específico grupo de seguridad.
11	Photo **[**Foto**]**	La ruta de acceso para la foto del empleado.
12	Signature **[**Firma)	Una opción para trabajar con una almohadilla para firmas que soportan el protocolo Wintab a fin de coger la firma del empleado (además del hardware, una licencia especial del Falcon es también requerida), o trabajar con un dispositivo TWAIN semejante a la pantalla **Capture Photo [**Capturar Foto**]**. Elija la ruta de acceso para la firma del empleado (solamente en la versión PRO).
13	System Report **[**Informe del Sistema**]**	Un informe mostrando las puertas activas para este empleado.

Ref.	Nombre del campo	Descripción
14	Add Trn. **[**Agregar Transacción**]**	Permite agregar una transacción manual (será marcada en conformidad) para este empleado. Véase pantalla abajo: 
15	Print Details (Imprimir Detalles)	Imprime el contenido de las 4 fichas en una página.

4.1.1.1 Administración

Consiste en los datos que pertenecen a la administración de la base de datos del empleado: número de ID, nombre, departamento (véase párrafo 4.2 Departamento & Compañía, en la página 25), posición, extensión, disposición de la tarjeta y otros datos relacionados a la tarjeta (asigne una de sus distribuciones predefinidas a esta tarjeta específica, véase párrafo 3.4.3 Editar Disposición de la Tarjeta (solamente en la versión PRO), en la página 18), correo electrónico, teléfono celular, comentarios.

También están incluidos varios parámetros para supervisión del empleado como sigue:

Fecha de Inducción – Anote la última fecha de re-certificación periódica de seguridad. La extensión del periodo es determinado en el campo **Enforce Induction Date [**Fecha de Imposición de la Inducción**]**, véase párrafo 3.3.3 Configuración de Comunicación, en la página 10. Una persona no es válida a menos que esté enlistada en este campo.

Fichadas Previstas – Un medio para supervisar las fichadas del empleado durante un periodo especificado. Para información adicional véase el párrafo Cuenta de Fichadas por Persona, en la página 54.

Última transacción – La última transacción del empleado es presentada aquí (véase párrafo 3.3.3 Configuración de Comunicación, en la página 10).

Fecha de Captura, Fecha de Emisión de la Tarjeta, Tarjetas Emitidas – La información es actualizada sistemáticamente cuando se han realizado estos procedimientos, y es usada para acompañar el proceso.

4.1.1.2 General

Información personal sobre el empleado, como dirección, cumpleaños, etc.

4.1.1.3 Detalles

Consiste en información administrativa adicional. También, es posible indicar la localización de un archivo de texto externo.

4.1.2 Sacar una Foto (solamente en la versión PRO)

El *Falcon PRO* permite sacar una foto de un empleado o de cualquier otro usuario de tarjeta para identificación final, y también preparar una tarjeta de empleado. Use un escáner o un capturador de imagen de video que soporte un interfaz TWAIN (así como la tarjeta Video Associates Labs VideoVue).
Esto puede ser hecho como sigue:

Escanear

Una foto puede ser escaneada y guardada en su PC y después insertada en su archivo del empleado.

Paso 1. Asegúrese que los dispositivos de hardware/software para escanear estén disponibles en su sistema.

Paso 2. Haga clic en la fila del empleado relevante.

Paso 3. Coloque la foto requerida en su escáner. Haga clic en el botón **Capture**, usted puede hacer clic en el botón derecho del ratón en **Grab picture** y elegir el dispositivo de captura requerido. Escanee la foto y guárdela, la foto será colocada en el archivo del personal bajo la fila seleccionada, además de ser guardada en el directorio **Photos [Fotos]**.

Importar un archivo de fotos existente

Usted puede usar una foto de un archivo JPG o BMP existente, como sigue:

Paso 1. Al hacer doble clic en la fila del empleado, la pantalla **Employee Details** aparecerá.

Paso 2. En la sección **Photo** haga clic en el icono, ubique el archivo guardado y haga clic en **Open**.

Pegar una foto existente de su portapapeles

Si un archivo BMP es almacenado en el portapapeles, usted puede pegarlo en su pantalla **Capture photo** (CTRL+V), después de haber hecho clic en el botón **Capture**.

4.1.3 Imprimir una Tarjeta (solamente en la versión PRO)

Paso 1. Para imprimir una tarjeta haga clic en **Print card [**Imprimir Tarjeta**]** en el archivo **Personnel**.

Paso 2. Elija la impresora relevante y haga clic en **Print**.

4.2 Departamento & Compañía

Usted puede agregar un departamento o una compañía haciendo lo siguiente:

- Vaya al menú **Personnel** | **Department and Company**, haga clic en el botón **New** y anote un nombre de departamento, O
- Vaya a **Employee Details | Management** o **Visitors | Visitor Details** y simplemente anote un nombre de Departamento / Compañía.

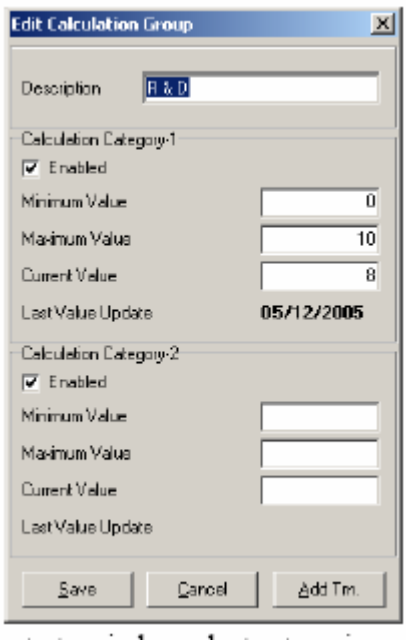
Los departamentos serán asignados a los empleados, las compañías serán asignadas a los visitantes.

Nota: *Los cambios realizados a estas bases de datos no serán abarcadores (es decir: si usted cambia un nombre de departamento, usted tendrá que hacer eso para todos los empleados que fueron asignados a este departamento).*

4.3 Grupos de Cálculo

Definir grupos de cálculo

Un grupo del cálculo es una posibilidad para categorizar un grupo de usuarios del recurso. Estos grupos pueden ser administrados y supervisados, y pueden ser emitidos informes por grupo; la pantalla siguiente aparece cuando usted edita un grupo:



Cada grupo del cálculo consiste en hasta dos categorías independientes.

Paso 1. Llene el campo **Description** para nombrar a su grupo de cálculo.

Paso 2. Para habilitar la limitación de la cuenta, usted debe definir un **Minimum Value [**Valor Mínimo**]** y un **Maximum Value [**Valor Máximo**]**.

El botón **Add Trn**. permite agregar una transacción manual que será actualizada para todos los empleados que estén asignados al grupo de cálculo específico, es decir: Si todos los empleados han acabado el trabajo, es posible informar Salida para todos inmediatamente.

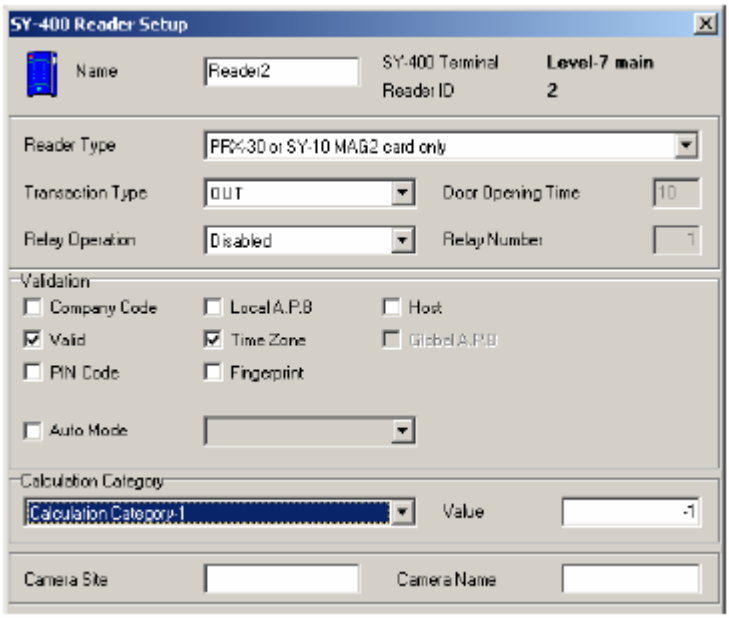
Asignar a un empleado

Vaya a: en la pantalla **Employee Details** sob **Management** seleccione el **Calculation Group** relevante.

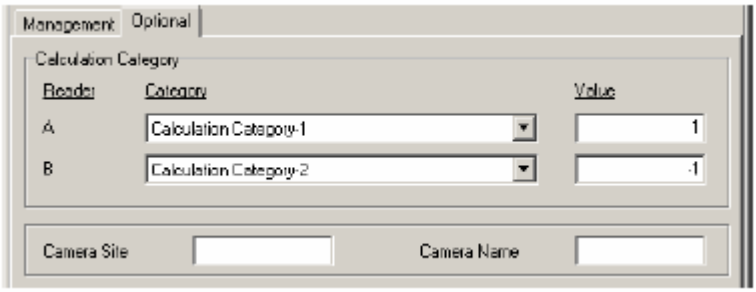
Asignar categorías de cálculo a lectoras relevantes

Las categorías de cálculo pueden ser asignadas a cada lectora como sigue:

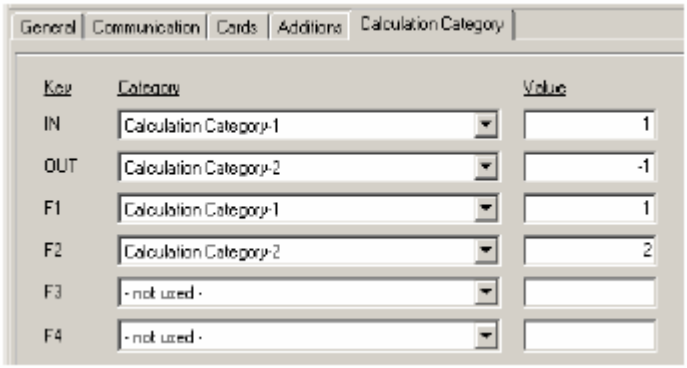
- SY-400



- Acceso
  Generalmente la lectora A es usada para Entrada y la lectora B para Salida.



- COM-II-PRO
  Cada tecla de función puede ser asignada a una distinta categoría de cálculo.



Capítulo 5 – Operación de Rutina

Después de haber sido establecido el procedimiento de configuración, hay actividades regulares que implican en la codificación de datos en las diversas carpetas como sigue:

5.1 Calendario

El calendario fue desarrollado e incorporado al sistema *Falcon* para conceder mayor flexibilidad al usuario definiéndose parámetros de acceso más amplios. Además de su flexibilidad, el **Calendario** permite programación a largo plazo.

El *Falcon* permite definir y programar cada día del año con parámetros de acceso específicos para horas y días irregulares, como por ejemplo: feriados, fines de semana.

Las mismas zonas de tiempo pueden ser utilizadas cada año; en caso de que sean requeridos ajustes estos son actualizados en la carpeta **Calendario**.

En el pasado, el acceso era definido:
Fecha >>Día de la Semana>>Horas de Acceso

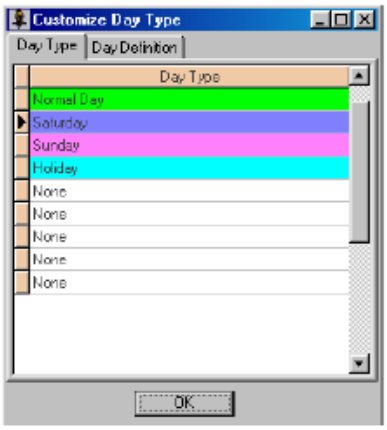
Actualmente el acceso es definido:
Fecha >>> Tipo de Día >>> Horas de Acceso

Los terminales SY-400 y Master reciben información del calendario y la usan para la configuración de las Zonas Horarias y el Auto Modo.

Definiendo un tipo de día
Una definición de tipo de día se aplica a días completos o medio-días de vacaciones y a otros días excepcionales. El sistema soporta 9 tipos de días de trabajo. Un Master usa apenas los siete primeros días.

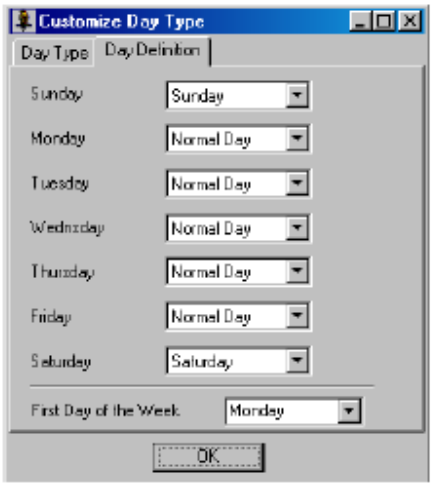
Paso 1. Entre a **Setup** a través del menú. Haga clic en la opción **Calendar [**Calendario**]**. Aparece la pantalla **Calendar**.

Paso 2. En el menú haga clic en el botón **Customize [**Personalizar**]** y después en **Day Type [**Tipo de Día**]**; aparece la pantalla **Day Type** (abajo).



Paso 3. Haga clic en la ficha **Day Type**. En la pantalla **Day Type** usted puede añadir o cambiar el tipo de día requerido y la indicación de color del día (Cada día ya está señalado en colores). Usted puede cambiar el colorido haciendo doble clic y seleccionando otro color. Haga clic en **OK**.

Definición de Día
Permite establecer una definición predeterminada de tipo de día para cada día de la semana.



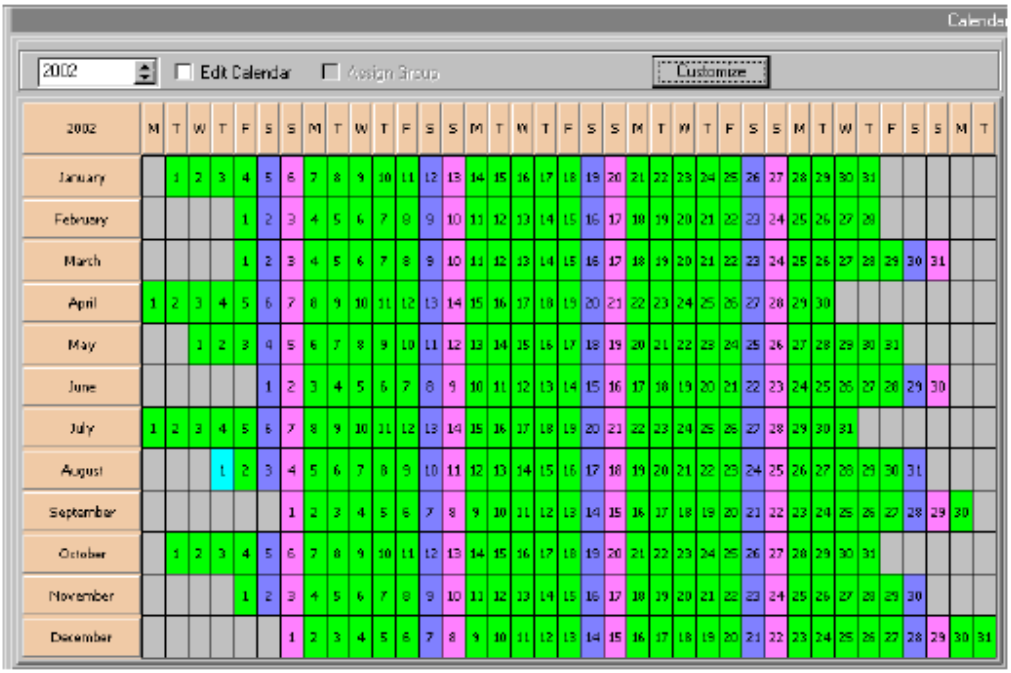
Paso 1. Haga clic en la ficha **Day Definition [**Definición de Día**]**.

Paso 2. Elija el primer día de la semana, después entre el tipo de día para cada día de la semana; esta será la definición predeterminada del sistema.

Paso 3. Entre el año que quiere definir.

Paso 4. Para cambiar un único tipo de día, señale la casilla de verificación **Edit Calendar [**Editar Calendario**]** en la pantalla **Calendar**.
El Calendario muestra los días codificados en colores que usted ha programado. Aquí usted puede continuar y elegir días especiales y días feriados.

Paso 5. Señale la casilla de verificación **Assign Group [**Asignar Grupo**]**, y seleccione un tipo de día. Después haga clic en todos los días a ser asignados al tipo específico de día que usted acaba de seleccionar. El color de los cuadrados cambia respectivamente.



5.2 Auto Modos

Esta carpeta, que es usada para terminales Master y SY-400, define el modo de entrada de los terminales. El terminal cambiará su modo de operación según la fecha y hora específicas.

5.2.1 Auto Modo para terminales Master

La pantalla **Master Auto Mode [**Auto Modo Master**]** es dividida en dos fichas principales:

Auto Mode List [Lista del Auto Modo**]** y **Auto Mode Detail List [**Lista Detallada del Auto Modo**].**

Cada Auto Modo consiste en una o más líneas de definición.

5.2.1.1 Lista Auto Modo

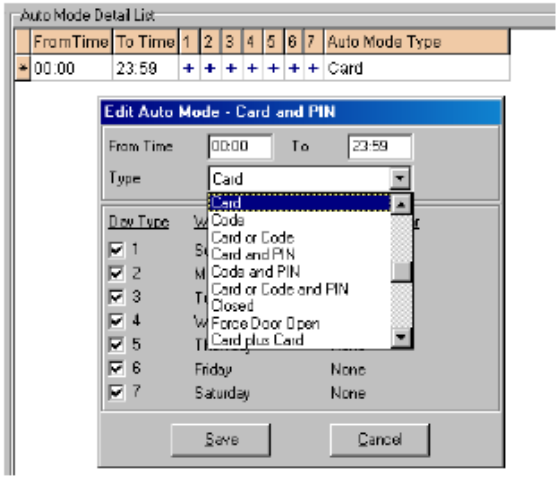
La **Auto Mode List** permite transición automatizada entre una combinación de modos de acceso predefinidos.

5.2.1.2 Lista de Detalles del Auto Modo

La **Auto Mode Detail List** es para definir parámetros de hora y día, dedicados a **Medidas de Seguridad de Acceso** particulares.

A seguir presentamos los modos de acceso predefinidos:

Card [Tarjeta**]** – solamente por tarjeta
Code [Código**]** – por nombre de empleado
Card and Code [Tarjeta y Código**]**
Card and PIN [Tarjeta y PIN**]** – + un código adicional
Code and PIN [Código y PIN**]**
Card or Code and PIN [Tarjeta o Código y PIN**]**
Closed [Cerrada**]** – No es permitida la entrada
Force Door Open [Abertura Forzada de Puerta**]** – Constantemente abierta
Card plus card [Tarjeta más tarjeta**]** – Entrada con un acompañante



5.2.1.3 Definir Auto Modo

Usted puede definir un Auto Modo para un terminal Master con o sin utilizar el Calendario.

Para programar el Auto Modo usando el Calendario, usted debe primero entrar a **Setup | Terminal List**, hacer doble clic en un Master, después hacer clic en la ficha **Additions** y en el botón de radio

Yes en el área **Use calendar [**Usar Calendario**]**. Para programar un Auto Modo para un Master, haga clic en **Auto Mode**; aparece la pantalla **Auto Mode** (arriba).
En los campos **From Time [**Desde la Hora**]** y **To Time [**Hasta la Hora**]** defina el rango de hora en la cual el **Auto Mode** será ejecutado.

En los campos 1 a 7 defina el tipo de día por el cual las condiciones programadas irán a operar.

En el campo **Auto Mode Type [**Tipo de Auto Modo**]**, entre el tipo de Auto Modo que desea usar.

Nota: *Asegúrese que todo el rango de 24 horas está totalmente dividido en zonas horarias. Por ejemplo:*

00:00-06:00- Tarjeta + código
06:00-18:00- Código
18:00-23:59- Tarjeta + código

En el ejemplo abajo cada número y el correspondiente campo debajo representan un tipo de día. El primer tipo de día en este ejemplo es "Día Normal" que representa de Lunes a Viernes.

Desde la Hora	Hasta la hora	1	2	3	4	5	6	7	Auto Modo
6:00	18:00	+	-	-	-	-	-	-	Código

Para programar un **Auto Modo** sin usar el Calendario entre a **Setup | Terminal List**, haga clic en **New [**Nuevo**]** en la parte inferior de la pantalla, después haga clic en **Additions**, y clic en el botón de radio **Without Calendar [**Sin Calendario**]**. En este caso, la definición de un acceso de entrada entre las horas **6:00 -18:00** para todos los días, excluyendo Sábado y Domingo será exhibida como se ve a seguir:

Desde la Hora	Hasta la hora	1	2	3	4	5	6	7	Auto Modo
6:00	18:00	-	+	+	+	+	+	-	Código

5.2.2 Auto Modo para SY-400

Es más fácil unir un auto modo a un tipo de día pues las diferencias son visibles.

Paso 1. Haga clic en la ficha **SY-400**. Para añadir un nuevo auto modo haga clic en **New**; una nueva línea es agregada a la columna **Auto Mode List**, anote el nombre apropiado.

Paso 2. En el gráfico **Auto Mode Details** señale la casilla de verificación **Edit [**Editar**]**, y asegúrese de estar usando el tipo relevante de auto modo. Haciendo clic y arrastrando el ratón, señale los días y horas que quiere definir (el gráfico es compuesto de unidades de tiempo de 30 minutos).

Nota: *Mientras pasa el ratón por el gráfico, usted puede ver su exacta ubicación, indicada en la parte inferior del gráfico (tipo de día, hora y modo de acceso).*

Modos de acceso:

Default [Predeterminado**]** – Correspondiente a las definiciones de validación de la lectora.
Card [Tarjeta**]**
Card and PIN [Tarjeta y PIN**]**
Card and finger [Tarjeta y Dedo**]**
Card+PIN+Finger [Tarjeta+PIN+Dedo**]**
Card plus Card [Tarjeta más Tarjeta**]**
Force door open [Abertura Forzada de Puerta**]** – El relé está activo todo el tiempo (véase definición de la lectora).
Closed [Cerrada**]** – La lectora está desactivada.

5.3 Lista de Terminales

Este módulo permite definir los parámetros de control de acceso del sistema para todos los terminales (Master, SY-400, COM-II-PRO, alarma) y sus lectoras como sigue:

Nota: *Usted puede copiar un terminal incluyendo sus lectoras subordinadas haciendo clic con el botón secundario del ratón en el relevante terminal en su lista de terminales.*

5.3.1 Definir un Terminal Master

Paso 1. En el menú elija **Setup**.
Paso 2. En **Module List** elija el archivo **Terminal List**.
Paso 3. Haga clic en la ficha **Master** + **Access** en la pantalla **Terminal List**.
Paso 4. Haga clic en **New** en la parte inferior de la pantalla; la pantalla **Terminal Setup -Master** aparece incluyendo cuatro fichas.

General

Paso 1. Elija la ficha **General** y anote el **ID** y el **Name** del terminal.

Paso 2. En el campo **Trans File Name [**Archivo de Transicción**]** elija el nombre del archivo de texto de la destinación a la cual la transacción será exportada.

Paso 3. En el campo **Format [**Formato**]** seleccione **Master** o cualquier otro formato apropiado que aparece en la lista desplegable.
Normalmente, esto ya deberá estar hecho en la configuración inicial del sistema.

Communication [Comunicación**]**

Paso 1. Elija la ficha **Communication**.

Paso 2. En la sección **Connection Type [**Tipo de Conexión**]** elija un tipo de comunicación:

Local – El puerto COM y la velocidad en baudios deben estar definidos.

Modem – Entre el número de teléfono y una cadena Init. opcional.

Network (**Red**) – comunicación TCP/IP – entre la dirección y el Puerto en uso (generalmente 3734).

Cards [Tarjetas**]**

Paso 1. En el campo **Cards | Start from** entre el número de colocación desde el cual un número de tarjeta será leído al archivo **Transaction [**Transacción**]**.

Paso 2. En el campo **Length [**Extensión**]** anote la extensión del número (de izquierda a derecha).

Additions [Adiciones**]**

Duress Code [Código de Amenaza**]** – El código de emergencia que permite acceso a todas las tarjetas, mientras registra un evento del tipo "Código de Amenaza".

Max Cards [Máx. Tarjetas**]** – Indica la cantidad máxima de tarjetas permitidas.

Nota: *Para Master-128 no anote un valor que ultrapase 2976.*

Para Master-512 no anote un valor que ultrapase 14000.

Activate Anti-Pass-Back [Activar Contra Nueva Fichada**]** – Impide que una tarjeta sea fichada dos veces en la misma lectora. Permite contra nueva fichada para todas las lectoras que pertenecen a un Master específico.

Send offline lists to Access units [Enviar listas a las unidades de Acceso cuando Desconectado**]** – Listas autorizadas pueden ser señaladas y enviadas a las unidades de Acceso, para permitir abertura de puerta independientemente de comunicación con el Master.

Nota: *A partir de la versión Master 3.20 y para las lectoras compatibles*.

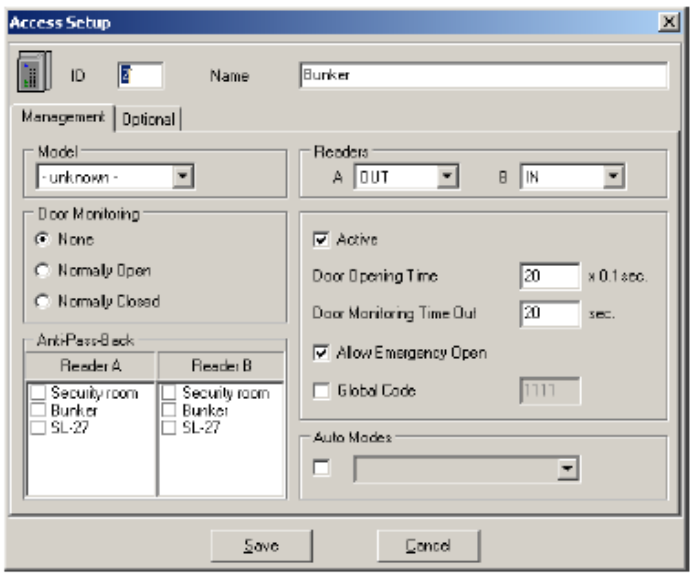
Use Calendar [Usar Calendario**]** – Indica si el Master soporta un calendario (La primera versión Master firmware que soporta el uso del calendario es la 3.15).

Relay Logic [Relé Lógico**]**– Una posibilidad de usar un archivo externo de configuración que contiene definiciones lógicas de transmisión. El usuario puede definir cuales los eventos que serán enviados cuando la Entrada/Salida cambia. Para mayores instrucciones para escribir un archivo de configuración refiérase a la Documentación del *Phantom* (RelayLog.txt).

Automatic Data Send [Envío Automático de Datos**]** – Al trabajar con un Servidor SY: a partir de la versión firmware 2.22, transacciones y consultas pueden ser iniciadas a cada par de segundos en el modo En Línea, o no iniciadas en el modo sin conexión.

5.3.2 Definir una Lectora de Acceso

Management [Administración**]**



Paso 1. Entre al modo **Setup** y haga clic en **Terminal List**. Haga clic en el archivo **Master**.

Paso 2. En la pantalla **Access list** haga clic en **New**; la pantalla **Access Setup** aparece.

Paso 3. En la pantalla **Access Setup** complete el campo **ID**. En el campo **Name** entre un nombre de su elección para representar la locación de la lectora. En el campo/s **Reader**/s entre el modo relevante.

Nota: *Cuando una lectora es señalada como **None**, todas las transacciones de aquella lectora serán almacenadas en el archivo Rejected.nnn.*

Paso 4. Bajo **Model [**Modelo**]** elija cual controlador será usado.

La sección **Door Monitor [**Monitor de la Puerta**]**, predeterminada como **None**, controla el estatus de **Open/Close [**Abierto/Cerrado**]** de un sensor de puerta.
Dependiendo del tipo de sensor de puerta a su disposición, usted puede tener su sensor en la posición **Normally Closed [**Generalmente Cerrado**]** o **Normally Open [**Generalmente Abierto**]** para hacerlo operable.

Door Opening Time **[**Tiempo de Abertura de la Puerta**]** – Define el intervalo de tiempo en que el relé de la puerta permanecerá abierto, en unidades de 0.1 segundos.

Door Monitoring Time out **[**Tiempo de Espera para Monitorear la Puerta**]** – Define el periodo máximo de tiempo (en seg.) en el cual es permitida la abertura de la puerta, antes de ser activada la alarma.

Allow Emergency Open **[**Permite Abertura de Emergencia**]** – Señalando esta casilla de verificación, se permite la abertura de la puerta durante una emergencia. Para más informaciones, véase el Capítulo 13 – Localización, en la página 67.

Global Code **[**Código Global**]** – Cuando la lectora de Acceso está en el modo Tarjeta+PIN y un empleado no tiene un código PIN individual, este código es usado en cambio. Así, un grupo específico de empleados que conocen este código pueden usarlo para entrar en aquella puerta.

Bajo Auto Modes – Permite seleccionar un auto modo predeterminado: véase 5.2 Auto Modos, en la página 30. Esto puede ser hecho solamente entre lectoras de Acceso que pertenecen al mismo terminal Master, siempre que la casilla de verificación **Activate Anti-Pass-Back** esté señalada bajo las definiciones del Master.

Para cada Acceso, haga una lista de todas las lectoras administradas por el mismo terminal, y determine desde que lectora el acceso es permitido. Una tarjeta que sea fichada en la lectora actual será permitida solamente si la lectora anterior estaba señalada en la pantalla **current reader set-up [**configuración de la lectora actual**]**.

Nota: *Si no fue señalada ninguna lectora en la lista, el acceso no será permitido a través de esta lectora.*

De eso modo, es posible:

- Impedir entrada no-autorizada, rechazando 2 continuas entradas/salidas a través de la misma lectora.
- Definir co-dependencias de acceso entre las lectoras para habilitar el encaminamiento de empleados en el sitio.

Usted debe establecer definiciones de permisión por lectora, a través de cual lectora será permitido el paso. Por ejemplo: Para habilitar el acceso a través de una lectora específica, usted debe definir al revés: si usted desea permitir el paso vía una lectora usted debe marcarlo en la lectora donde el paso “chrono-wise” viene antes de ella.

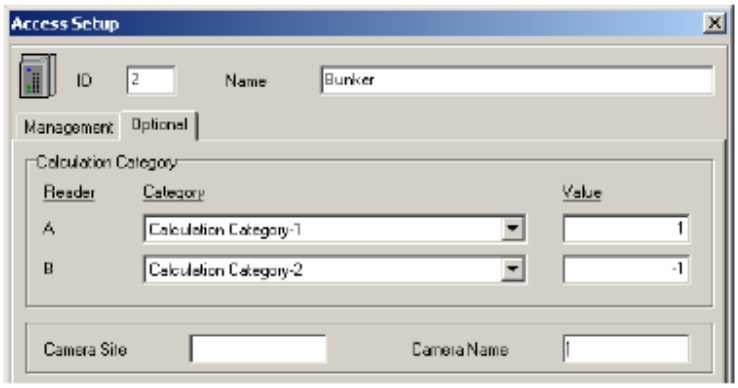
Por ejemplo:

Para habilitar el paso de la Lectora A a la Lectora B, a la Lectora C y de vuelta a la Lectora A, señale como sigue:

En la pantalla Reader A Setup:	**En la pantalla Reader B Setup:**	**En la pantalla Reader C Setup:**
Lectora C	Lectora A	Lectora B

Del mismo modo, usted debe definir todas las otras lectoras.

Optional [Opcional**]**



Para definir una **Calculation Category [**Categoría de Cálculo**]**, véase 4.3 Grupos de Cálculo, en la página 25.

Camera site (solamente en la versión PRO) – El nombre del servidor de cámara asociado con las lectoras, que está integrado al sistema CCTV (caso sensitivo).

Camera name (solamente en la versión PRO) – El nombre de la cámara asociado a la lectora específica (caso sensitivo).

5.3.3 Definir un Terminal SY-400

Paso 1. En el menú o en la barra de herramientas elija **Setup**. En **Module List** elija el archivo **Terminal List**.

Paso 2. Haga clic en la ficha **SY-400** en la parte superior de la pantalla **Terminal List**. Haga clic en **New**; la pantalla **Terminal Setup SY-400** aparece incluyendo los siguientes archivos:

General

Paso 1. Elija la ficha **General** y anote el **ID** y el **Name** del terminal.

Paso 2. En el campo **Transaction File [**Archivo de Transicción**]** elija el nombre del archivo de texto de la destinación al cual la transacción será exportada.

Paso 3. Seleccione el formato relevante en el cuadro combinado **Format [**Formato**]**.

Paso 4. El campo opcional **Query File [**Consultar Archivo**]** será usado como un campo auxiliar para escribir consultas (una característica avanzada).

Communication [Comunicación**]**

Paso 1. Elija la ficha **Communication**.

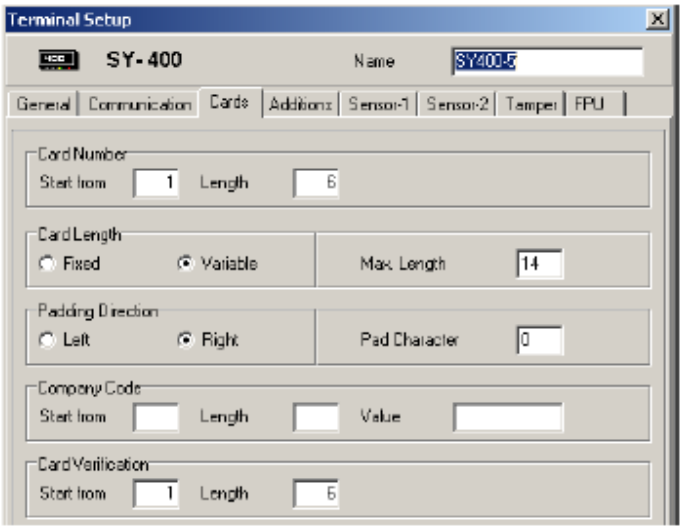
Paso 2. En la sección **Connection Type [**Tipo de Conexión**]** elija un tipo de comunicación:

Local – El puerto COM y la velocidad en baudios deben estar definidos.

Modem – Entre el número de teléfono y una Cadena Init. opcional. (Al usar el estándar de Synel empotrado en el ISOMODEM usted puede anotar en la Cadena Init predefinida:&FE0V1)

Network [Red**]** – comunicación TCP/IP – entre la dirección y el puerto en uso (generalmente 3734).

Cards [Tarjetas**]**



Paso 1. Elija la ficha **Cards**. En el campo **Start from [**Empezar de**]** anote el número de colocación de donde un número de tarjeta es leído al archivo **Transaction [**Transacción**]**.

Paso 2. En el campo **Length [**Extensión**]** anote el número de extensión (de la izquierda a la derecha).

Paso 3. En la sección **SY-400**, señale **Fixed [**Fijo**]** o **Variable**. Para Variable usted debe además definir los parámetros **Padding [**Rellenar**]**. Después, en el campo **Max. Length** [Máx. Extensión] entre el número máximo de dígitos a ser leído. Si es usado un número fijo el **Padding** no será operable.

Paso 4. En la sección **Company [**Compañía**]**, los campos **Start from** [Empezar de] y **Length [**Extensión**]** permiten verificar un código predeterminado de tarjeta. El campo **Value [**Valor**]** es para verificar el Número de la Compañía (o Dept. Grupo, etc.) dentro del Número de la Tarjeta.

Paso 5. La sección **Verification [**Verificación**]** es para verificar los datos de la tarjeta. En el campo **Start from** anote un número que signifique cual será el dígito a verificar. En el campo **Length** entre el número de dígitos a ser verificado.

Si en una empresa particular hay cuatro departamentos (o cuatro filiales), cada departamento puede ser definido por un conjunto de números (un valor). Estos números serán añadidos al número del empleado. Así, una Tarjeta de Acceso puede ser contener dos números, uno asignado al departamento y otro asignado a una particular tarjeta de acceso.

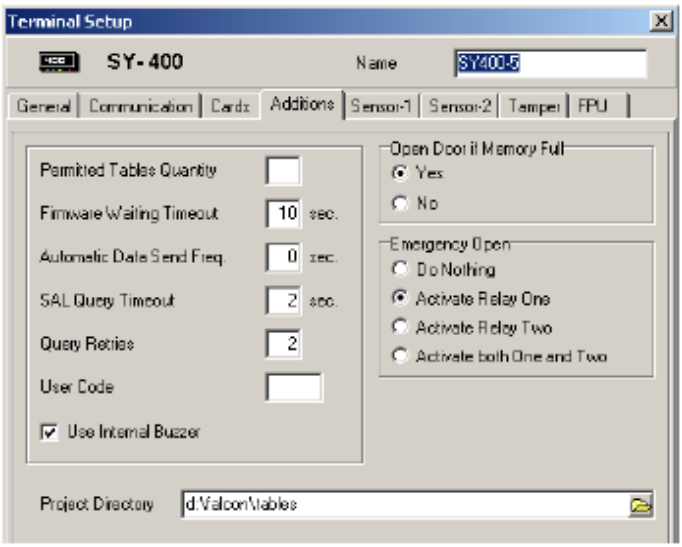
Al **Padding** un número complete los espacios de dígitos requeridos para un número apropiado (identificable por la lectora. Padding es necesario cuando un número de tarjeta contiene menos dígitos que la extensión total definida en la pantalla **Terminal Setup**.

Ejemplo: Tarjeta de Acceso No. 300564798823XX

No. de ID del Departamento	**Tarjeta Individual no.**	**Rellenar**
300564798823	300564798823XX	300564798823 XX

Se recomienda clasificar este código como un cliente, no un código de departamento. Cada organización recibirá un código único compartido por todos los departamentos.

Additions [Adiciones**]**



Permitted Tables Quantity [Cantidad de Tablas Permitida**]** – Es el número permitido de tablas de acceso enviadas al terminal.

Firmware Waiting Timeout [Tiempo de Espera Firmware**]** – El número de segundos desde el último pedido del host antes de dar la respuesta "No Host" al SAL. El terminal entonces pasa al modo offline y retornará al modo en línea solamente en la próxima consulta del host. Usado solamente para comunicación serial. El tiempo de espera recomendado es de 5 segundos.

Automatic Data Send Freq. **[Frec. Envío Automático de Datos]** – La frecuencia del envío de Datos del terminal al host (frecuencia del intervalo de interrogación para la comunicación TCP/IP) en segundos. 0 = El terminal no iniciará el envío de datos al host. Consultas no son afectadas por este parámetro y son inmediatamente enviadas al host.

SAL Query Timeout [Tiempo de Espera de Consulta al SAL**]** – El número de segundos que el SAL espera por una respuesta después de enviar una consulta al host. El tiempo de espera recomendado es: 2 segundos. **SAL Query Timeout** x **Query Retries** deberá ser inferior al **Firmware Waiting Timeout**.

Query Retries [Reintentar Consultas**]** – Cuantas veces el SAL intentará consultar el host.

User Code [Código de Usuario**]** – Un código definido de usuario que puede ser usado para definir el terminal, dependiendo de la aplicación que es activada en el terminal.

Use Internal Buzzer [Usar Zumbador Interno**]** – Determina si el zumbador interno del controlador será activado cuando ocurrir un error.

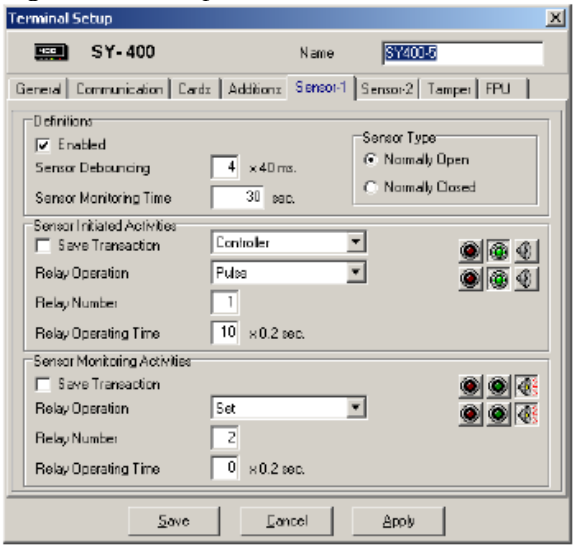
Open door if memory is full [Abrir puerta si la memoria está llena**]** – haga clic en el botón de radio **Yes/No**.

Emergency open [Abertura de emergencia**]** – Durante un evento determina como los relés del SY-400 irán a reaccionar

Project Directory [Directorio del Proyecto**]** – Esta es la localización de las tablas de programación del terminal.

Sensors [Sensores**]**

A partir de la versión firmware 6.000, el SY-400 tiene tres sensores: el tercer sensor es usado como un conmutador de tamper. En las versiones anteriores hay dos sensores, el sensor 2 está eléctricamente conectado al relé 2, por consiguiente es siempre activado cuando el sensor 2 está ON.



Los sensores son administrados como sigue:

1. **Definitions [**Definiciones**]:**
   Enabled **[**Habilitado**]** – Habilita/Deshabilita el sensor
   Sensor debouncing **[**Recuperación del Sensor**]** – Tiempo de espera para que el sensor se estabilice.
   Sensor monitoring time **[**Tiempo de monitoreo del sensor**]** – Alerta si el sensor ha estado activo por más tiempo que el tiempo definido (activa la sección **Sensor Monitoring Activities [**Actividades de Monitoreo del Sensor**]** abajo).
   Sensor type **[**Tipo de sensor**]** – Normally open **[**Normalmente abierto**]** (el circuito es desconectado y el sensor causa corto circuito) o Normally closed **[**Normalmente cerrado**]** (el circuito es cortado por predeterminación y el sensor lo desconecta).
2. **Sensor Initiated Activities [**Actividades Iniciadas por el Sensor**]:**
   Save Transaction **[**Guardar Transacción**]** – Si crear una indicación de evento para operación del sensor. Elija del cuadro de lista si el evento será escrito con la ID del controlador o una ID de lectora.
   Relay operation **[**Operación del Relé**]**: Pulso, Deshabilitado, Establecer, Reestablecer
   Relay number **[**Número del relé**]** – Entre **1** o **2**. Si desear elegir ambos, entre **0**.
   Relay operating time **[**Tiempo de operación del relé**]** – Tiempo para activación del relé en 1/5 segundos.
   LED buttons **[**botones LED**]** – Presione un LED/s para operar cuando el sensor está activo.

3. **Sensor Monitoring Activities [**Actividades de Monitoreo de Sensor**]**: guardar una transacción cuando el sensor permanece activo por más tiempo que el tiempo de monitoreo definido (Por ejemplo, si la puerta estuvo abierta por más tiempo que el tiempo definido), y también guardar una transacción cuando el sensor fue cerrado después de estar abierto por tiempo demasiado.
   Save Transaction [Guardar Transacción] – Si crear una indicación de abierto-por-demasiado-tiempo/cerrado-después-de-abierto-por-demasiado-tiempo para operación del sensor. Si el modo seleccionado **Relay Operation** es **Set**, al cerrar el evento, el relé será **Reset** (i.e.: activar un zumbador cuando la puerta está abierta por mucho tiempo).
   Los otros parámetros son idénticos al **Sensor Initiated Activities**.

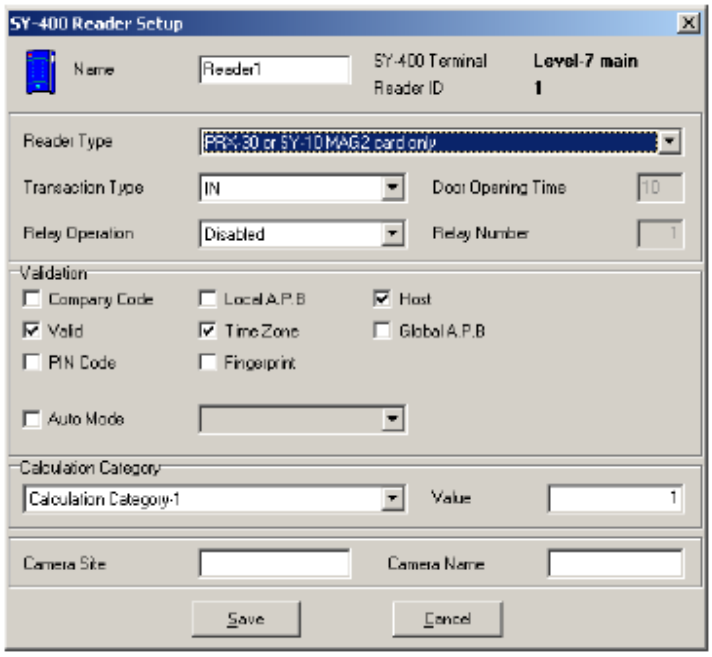
FPU

FPU Mode SYServer **[**Servidor SY Modo FPU**]** – En verificación: Si falta una plantilla: En el modo Master, su terminal puede enviar una consulta (usando el Servidor SY) para obtener la plantilla que falta desde el host. En el modo Slave, el terminal no consultará el PC sobre plantillas que faltan. El modo Slave es el modo predeterminado del terminal.

FPU Security threshold **[**Umbral de Seguridad FPU**]** – Aquí se define cuán estricta será la comparación de las huellas digitales. Very High **[**Muy Elevada**]** es muy estricta, Very Low **[**Muy Baja**]** no es tan estricta.

Request FPU Status **[**Solicitar Estatus del FPU**]** – Al obtener el estatus del terminal, se solicita también obtener el estatus de las huellas digitales de la unidad FP.

5.3.4 Definir una Lectora SY-400



En **Setup**, seleccione **Terminal List**, y haga clic en la ficha de la carpeta **SY-400**.

En la columna **Reader List [**Lista de Lectoras**]** en el lado derecho de la pantalla debe haber dos lectoras. Defina las lectoras como sigue:

Paso 1. Haga clic en **Reader 1** y entre el nombre de la Lectora.

Paso 2. En el campo **Reader Type [**Tipo de Lectora**]** elija las características operacionales de la lectora de la lista desplegable.

Nota: *Tablas no autorizadas serán enviadas a una lectora **Deshabilitada***!

Paso 3. En el campo **Transaction Type [**Tipo de Transacción**]** seleccione el modo de la lectora:
Ninguno – No guarda la transacción
IN – Entrada
OUT – Salida
Puerta – Define la transacción como Control de Puerta – Aparecerá en los informes, pero no en los informes de presencia.

Nota: *La combinación de lectoras tarjeta+teclado puede ser usada como una lectora de tarjetas o puede ser digitado un número.*

Paso 4. Elija una opción de la lista desplegable **Relay Operation [**Operación de Relé**]**.

Paso 5. En **Door Opening Time [**Tiempo de Abertura de la Puerta**]** anote el intervalo de tiempo en el cual el relé de la puerta será abierto (1/5 seg).

Paso 6. En el campo **Relay Number [**Número del Relé**]**. Entre **1** o **2**. Si desear elegir ambos, entre **0**.

Paso 7. En la sección **Validation [**Ratificación**]** en la parte inferior de la pantalla señale las opciones que quiere ratificar, como sigue:
Company Code **[**Código de la Compañía**]** – Un código (compañía/ dept. etc.) que es añadido al No. básico de la lectora (Como definido por el controlador).
Valid **[**Válido**]** – Los detalles personales en la lista autorizada.
Nota: *Tablas no autorizadas serán enviadas a la lectora si esta casilla de verificación no está señalada*.
Time Zone **[**Zona Horaria**]** – La tarjeta es autorizada a un específico intervalo de tiempo según las definiciones de la específica zona horaria.
Local Anti-Pass-Back – Ejecuta chequeos APB para tarjetas especificadas entre dos lectoras que pertenecen al mismo controlador, cuando un tipo es **In**, y el otro es **Out**.
PIN Code – Una medida adicional de seguridad que requiere la entrada de un código adicional. Un código de 4 dígitos debe ser digitado. La selección de auto modo lo cancela!
Fingerprint **[**Huellas Digitales**]** – Puede ser asignado a solamente una lectora. Debe ser señalado para operar la unidad de huellas digitales al usar auto modo. Una real verificación será realizada según el auto modo, si seleccionado!
Host – Verificación en línea usando el Servidor SY y un DLL especial (Por ejemplo: FlconDLL.dll).
Global Anti-Pass-Back – Ejecuta amplios chequeos APB del sistema vía el SYServer DLL.
Auto Mode – Permite seleccionar un auto modo preestablecido.

Paso 8. Haga clic en **Save [**Guardar**]**.

Paso 9. Para definir una segunda lectora repita este procedimiento.

5.3.5 Definir un Terminal COM-II-PRO

Paso 1. Para definir un reloj COM-II-PRO entre al modo **Setup** y haga clic en **Terminal List**.

Paso 2. Haga clic en la ficha de la carpeta **COM-II-PRO**.

Paso 3. Haga clic en **New** en la parte inferior de la pantalla; la pantalla **Terminal Setup** aparece.

Paso 4. En la parte superior, a la derecha, anote el nombre del terminal en el campo **Name**.

Paso 5. Haga clic en **General**, y teclee la ID del terminal en el campo **ID**.

Paso 6. En la carpeta **Communication [**Comunicación**]** elija el tipo de conexión apropiada y anote el restante de los campos, como requerido.

Paso 7. En la ficha **Cards [**Tarjetas**]** defina la posición del primer dígito del número de la tarjeta y también la extensión del número.

Paso 8. En la ficha **Additions [**Adiciones**]** anote el número, lugar y formato de los archivos de Transacciones.

Paso 9. En la parte inferior de la pantalla entre el nombre del directorio PEP que usted desea enviar al terminal. Haga clic en **Save [**Guardar**]** o **Cancel [**Cancelar**]**.

Note: *Repase el proyecto modelo Falcpep (sob el directorio Tablas) donde la primera lista de transacciones (creada por el terminal) debe estar en el formato de: Tarjeta, fecha, hora, llave. El primer archivo permitido debe estar en uno de los siguientes formatos (refiérase al contenido de la lista autorizada):*
Tarjeta – solamente tarjeta
Tarjeta, alfa – tarjeta y nombre
Tarjeta, alfa, alfa – tarjeta, nombre e ID.

Usted puede asignar diversas categorías de cálculo a este terminal según las teclas de función. Para más información, véase 4.3 Grupos de Cálculo, en la página 25.

5.3.6 Definir un Controlador de Alarma (solamente en la versión PRO)

El actualmente respaldado ProSYS 128 de Rokonet es un sistema de detección de alarma que se comunica con el *Falcon* como sigue:

- *Falcon* puede enviar la fecha y hora del PC al controlador.
- Las transacciones son colectadas solamente a través de la pantalla **Online [**En Línea**]**.

Paso 1. Para definir un controlador de alarma entre al modo **Setup** y haga clic en **Terminal List**.

Paso 2. Haga clic en la ficha de la carpeta **Alarm System [**Sistema de Alarma**]**.

Paso 3. Haga clic en **New** en la parte inferior de la pantalla; aparece la pantalla **Terminal Setup-Alarm Controller [**Configuración del Terminal – Controlador de Alarma**]**.

Paso 4. En la parte superior derecha de la pantalla, anote el nombre del terminal en el campo **Name**.

Paso 5. Entre la ID del terminal en el campo **ID**.

Paso 6. Seleccione el tipo/modelo del controlador de alarma.

Paso 7. En la carpeta **Communication [**Comunicación**]** elija el tipo de conexión apropiada y anote el restante de los campos, como requerido.

Paso 8. Usted debe deshabilitar el almacenamiento FIFO del puerto RS-232. De lo contrario el *Falcon* no podrá comunicarse con el controlador:
En Windows 2000: **My computer | Manage | Device Manager | Ports | Communication port COM X | Properties | Port Settings | Advanced**
En Windows NT: **Controller Panel | Ports | COM X | Settings | Advanced**
En Windows 95: **My computer | Properties | Device Manager | Ports | Communication port COM X | Properties | Port Settings | Advanced**

5.3.7 Definir un Detector de Alarma

Paso 1. Entre al modo **Setup** y haga clic en **Terminal List**. Haga clic en la ficha **Alarm System [**Sistema de Alarma**]**.

Paso 2. En la pantalla **Detector list [**Lista de Detectores**]** haga clic en **New**; la pantalla **Alarm Detector Setup [**Configuración del Detector de Alarma**]** aparece.

Paso 3. Anote un **ID** y **Name**. El **Nombre** de su elección para representar la ubicación del detector.

5.4 Definir una Zona Horaria

El módulo Zona Horaria controla y define los rangos de tiempos de control de acceso de los terminales Master y SY-400 por tipo de día, como sigue:

5.4.1 Definir una Zona Horaria para un Terminal Master

El terminal Master puede definir hasta 15 Zonas Horarias por Acceso (99 Zonas Horarias diferentes por unidad Master), con o sin el uso del Calendario. Para elegir o cancelar la función calendario entre a la carpeta **Terminal List**. Haga clic en la ficha **Additions [**Adiciones**]** y elija **With Calendar [**Con Calendario**]** o **Without Calendar [**Sin Calendario**]**.

Paso 1. Después de entrar a **Setup** haga clic en el Módulo **Time Zone [**Zona Horaria **]** en la lista de Módulos al lado izquierdo de la pantalla.

Paso 2. Haga clic en la ficha **TZ Master**.

Paso 3. Para añadir un nuevo **Access Group [**Grupo de Acceso**]** haga clic en el botón **New** en la parte inferior de la Lista de Zona Horaria; una nueva línea es añadida a la columna **Time Zone List [**Lista de Zona Horaria**];** anote el nombre apropiado.

Paso 4. Haga clic en el botón **Edit**, la pantalla **Edit Time Zone [**Editar Zona Horaria**]** aparece. Anote los campos con toda la información pertinente – rangos de hora y fecha para días especiales de la semana. Bajo **Access** señale el relevante botón de radio para permitir o bloquear el acceso en los días señalados.

Nota: *Semejante al* **Auto Modo** *cuando el calendario es usado, cada espacio representa un Tipo de Día, mientras sin el calendario, cada espacio representa un día de la semana*.

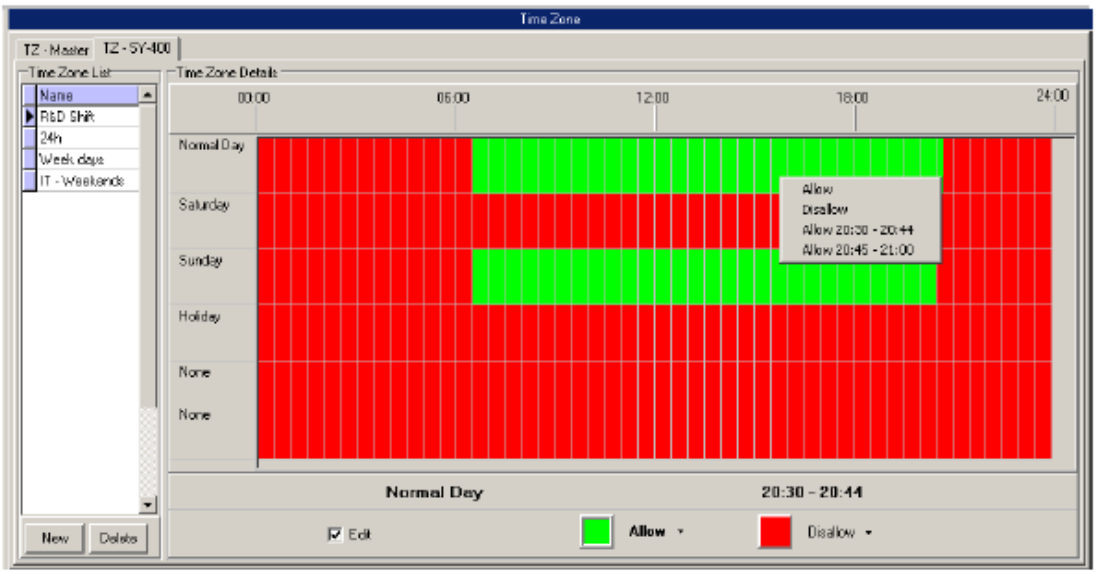
Al señalar el botón de radio **Yes** en la sección **Use Calendar** en la pantalla **Terminal setup**, para indicar que el calendario está siendo usado, apenas un tipo de día (cada uno de los números de 1-7 representa un tipo de día) debe ser marcado por un +.

Desde la hora	Hasta la hora	Desde la fecha	Hasta la fecha	1	2	3	4	5	6	7	Pass
6:00	18:00	1/1/02	7/1/02	+	-	-	-	-	-	-	+

Al señalar el botón de radio **No** en la sección **Use Calendar** en la pantalla **Terminal setup**, para indicar que el calendario no está siendo usado cada número representa un día de la semana, así todos los días regulares deben ser marcados por un a +:

Desde la hora	Hasta la hora	Desde la fecha	Hasta la fecha	1	2	3	4	5	6	7	Pass
6:00	18:00	1/1/02	7/1/02	-	+	+	+	+	+	-	+

5.4.2 Definir una Zona Horaria para el SY-400



Distinto del Master (usted puede o no usar el calendario para definiciones de zonas horarias), el SY-400 requiere la configuración de los parámetros del calendario.

Paso 1. Haga clic en la ficha **SY-400**.

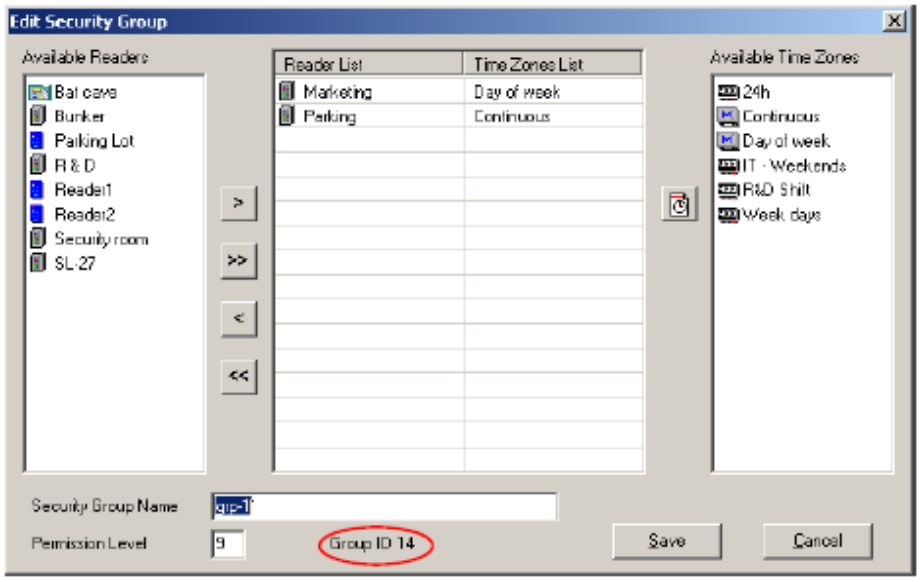
Paso 2. Para añadir una nueva **Time Zone** haga clic en el botón **New**; una nueva línea es agregada a la columna **Time Zone List**, anote el nombre apropiado.

Paso 3. En el gráfico Zona Horaria, haciendo clic y arrastrando el ratón, señale los días y horas que quiere definir. El gráfico es compuesto de unidades de tiempo de 30 minutos (hacer clic con el botón secundario del ratón le permite ajustar para unidades de 15 minutos si requerido). Señale la casilla de verificación **Edit**, y asegúrese de que está en el modo correcto (permitir y no permitir).

Nota: *Mientras pasa el ratón por el gráfico, usted puede ver su locación exacta indicada en la parte inferior del gráfico (tipo de día y hora).*

Nota: *La opción* ***Allow/disallow*** *permite cambiar el color. (Esto ya habia sido hecho previamente en la pantalla* **Options**).

5.5 Definir un Grupo de Seguridad



SY-400

Para los terminales SY-400 es posible asignar hasta 5 diferentes grupos de seguridad por empleado. La fecha de expiración es verificada solamente cuando las tablas son enviadas. Solamente grupos que no caducaron son usados.

Master

El Master puede retener un registro por empleado con una fecha de caducidad. Cuando dos grupos de seguridad se refieren al mismo terminal Master, el software elegirá la más próxima fecha de caducidad válida. Las zonas horarias serán emparejadas como sigue:

Para cada lectora (Acceso) es creada una lista interna de todas las zonas horarias activas. Si no existe una zona horaria activa para este empleado para esta lectora, entonces, el acceso será rechazado. Si no, la zona horaria con el ID más bajo (la lista de Zona Horaria del Master es organizada por ID ascendiente de zona horaria) será usada.

Este módulo permite asignar un grupo de seguridad a una Zona Horaria y a una puerta:

Paso 1. En la pantalla **Security Group [**Grupo de Seguridad**]**, haga clic en **New** y entre un nombre para el nuevo grupo de seguridad.

Paso 2. Defina el nivel de permisión para este grupo de seguridad. El nivel de permisión debe coincidir con el nivel de permisión del operador de supervisión relevante (para más informaciones véase el Capítulo 12 - Manutención, en la página 65 - Usuarios).

Paso 3. En el lado derecho de la pantalla, bajo **Security Group Details [**Detalles del Grupo de Seguridad**]** haga clic en **Edit** o doble clic en un grupo de seguridad en el campo **Security Group**.

Paso 4. La pantalla **Edit Security Group [**Editar Grupo de Seguridad**]** aparece. Todas las lectoras definidas serán listadas a la izquierda. A seguir, usted encontrará una tabla que permite asignar una zona horaria a una lectora. En el lado derecho está una lista de las zonas horarias actualmente definidas. Esta pantalla permite arrastrar y colocar datos entre las listas.

Nota: *Haciendo clic con el botón derecho del ratón en un grupo, es posible copiar el contenido de las definiciones del grupo a otro grupo (nuevamente clic con en botón derecho y pegar).*

Nota: *Lectoras inactivas no aparecerán en la lista de lectoras disponibles.*

5.6 Definir un Empleado

El archivo **Personnel [**Personal**]** permite rever toda la información general del empleado según diferentes ordenaciones. Esta base de datos puede ser actualizada en cualquier momento dado.

Nota: *Los datos pueden ser insertados directamente en la cuadrícula solamente cuando la casilla de verificación **Allow Grid Edit [Permite Editar Cuadrícula]** esté señalada.*

Un nuevo empleado puede ser añadido como sigue:

Paso 1. Haga clic en **Personnel, New**; la pantalla **Employee details [**Detalles del empleado**]** aparece.

Paso 2. Hojee por las fichas **Management, General**, y **Details** y anote la información relevante.

Nota: *Después de entrar el nombre del archivoe de fotografía, la fotografía aparece en la pantalla Personal*.

Paso 3. Haga clic en **Send Last [**Enviar el último**]** si desea actualizar el sistema con los datos particulares de un titular de tarjeta

Paso 4. Haga clic en **Send All [**Enviar todo**]** si desea enviar más de uno.

Paso 5. Señale cualquiera de los botones de radio que representan opciones para ordenar, según su elección.

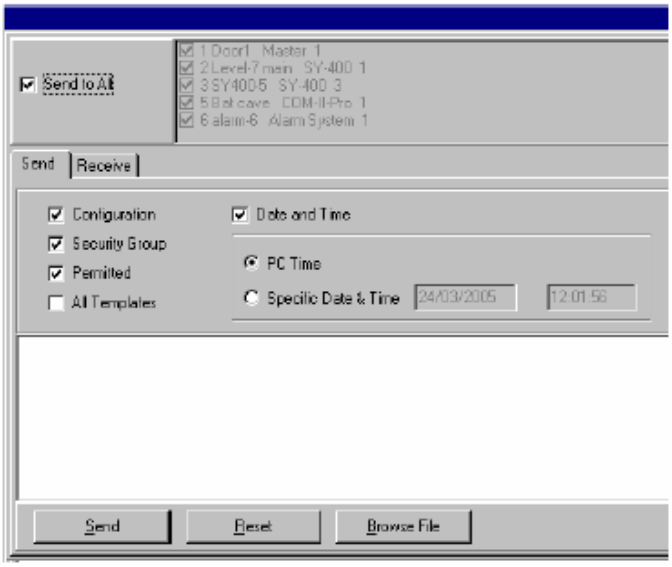
Nota: *Usted puede actualizar su pantalla usando el botón* **F5**.

Nota: *Al usar la opción* **Find** *una búsqueda incremental es activada*.

Para información elaborada en administración de empleados, véase el Capítulo 4 – Personal, en la página 21.

Capítulo 6 – Comunicación

Esta característica permite al usuario comunicarse con los terminales para enviar o recibir varias informaciones. En primer lugar usted debe elegir el control/s relevante/s (no señale la ficha **Send to All [**Enviar a Todos**]**). La ficha **Send [**Enviar**]** transfiere datos al control. Mientras la ficha **Receive [**Recibir**]** transfiere datos del control a la computadora (Estatus, nuevas transacciones, antiguas transacciones, lista autorizada) y determina qué datos serán recibidos y la localización del origen.



6.1 Enviar datos al terminal

Paso 1. Haga clic en la ficha **Send**.
Paso 2. Seleccione **Send to All** o un terminal específico.
Seleccione el tipo de datos que serán enviados.

Los siguientes datos pueden ser enviados:

Campo	**Descripción**
Date and Time **[**Fecha y Hora**]**	Fija una nueva fecha y hora en los terminales.
Configuration **[**Configuración**]**	Envía la configuración definida en la **Terminal List**.
Security Group (No aplicable para Com-II-PRO) **[**Grupo de Seguridad**]**	Envía todas las configuraciones definidas en las siguientes carpetas: **Security Groups, Time Zones, Auto Mode, Calendar**
Permitted Cards **[**Tarjetas Permitidas**]**	Envía la configuración definida en la carpeta **Personnel**.
All Templates (SY-400 solamente) **[**Todas las Plantillas**]**	Cuando no señalado: Solamente nuevas plantillas de huellas digitales son enviadas al terminal. Cuando señalado: La memoria de plantillas de huellas digitales en el terminal es limpiada y todas las plantillas autorizadas almacenadas en el PC son enviadas al terminal.

Nota: *Para SY-400: la lista autorizada incluirá a empleados que no han sido apuntados en una plantilla FP (pueden ser apuntados retroactivamente y enviados al terminal individualmente).*

Restablecer un terminal (solamente Master)

Esta operación inicia el terminal y causará que todos los datos de transacción (incluyendo los que no fueron colectados) sean perdidos permanentemente:

Seleccione **Send To All** o un terminal específico. Haga clic en **Reset**.

Browse File **[**Examinar archivo**]**

Permite ver los archivos LOG.

6.2 Recuperar datos desde el terminal

Paso 1. Haga clic en la ficha **Receive**. Seleccione **Send To All** o un terminal específico.

Paso 2. Seleccione el tipo de datos a recibir.

Campo	**Descripción**
Status **[**Estatus**]**	Abre una ventana que contiene la exhibición del estatus del terminal(s) y de las lectoras atribuidas.
Transactions **[**Transacciones**]**	Recibe nuevas transacciones del terminal(s). Los datos de la transacción pueden ser vistos en la tabla Transacción en el módulo Online.
Old Transactions **[**Transacciones antiguas**]**	Recolección de transacciones antiguas colectadas del terminal(s) junto con cualquier nueva transacción.
Permitted (Master Only) **[**Permitidas (Solamente Master**)**	Presenta una lista de todas las tarjetas actualmente almacenadas en la memoria del terminal

Registros con defecto serán colocados en el archivo Rejected.nnn (n=número del terminal). Si el archivo de transacción está con defecto y los datos no pueden ser registrados en el, la colección de datos será interrumpida. Bajo la ficha **Receive** usted encontrará el número de registros rechazados.

Capítulo 7 – Eventos

Además de transacciones regulares, el software del *Falcon* también permite la investigación retrospectiva de transacciones especiales, como por ejemplo: Tarjeta no válida más (expirada), acceso no permitido, etc. Estas transacciones especiales, llamadas eventos, pueden ser contorneadas por sonido y color, y pueden ser ordenadas en conformidad a eso.

Crear un Nuevo Evento

Haga clic en el botón **New Event [**Nuevo Evento**]**.
Defina todos los campos del **Event [**Evento**]**.

Editar una Línea de Evento

Seleccione el evento y haga clic en **Edit [**Editar**]** o, doble clic en una línea de evento habilita la edición.

Nota: *Usted puede marcar distintos eventos con distintos colores.*

Eliminar un Evento

Seleccione la línea del Evento.

Haga clic en el botón **Delete Event [**Eliminar Evento**]**.

La pantalla de definición de evento es compuesta de 4 fichas:

General – Iniciar el evento, y caracterizarlo.

Indication [Indicación**]** – Marcar el evento por color y sonido.

Automatic activity [Actividad automática**]** – Informar a una parte interna/externa sobre el evento vía SMS. Véase “SMS (solamente versión PRO)” en la página 16.

Operator instructions [Instrucciones al operador**]** – En caso de ocurrencia de un evento, instrucciones al operador.

El evento de tipo **Pass** se refiere a todas las transacciones válidas. Todos los tipos de transacciones excepto **Pass** pueden ser clasificadas como **All Exceptions** o requieren una definición específica.

Administración de evento

Todos los eventos actuales son presentados en la pantalla **Online [**En Línea**]**. Haciendo doble clic en una de las filas aparecerá la pantalla **Event notification [**Notificación de evento**]**.

General

Campo	**Descripción**
Description **[**Descripción**]**	Un texto libre donde el usuario puede caracterizar el evento
Event type **[**Tipo de Evento**]**	Un tipo de transacción irregular.
Active **[**Activo**]**	Un evento puede ser activo = funcional o cuando esta casilla de verificación no está marcada = no activo.
Card range **[**Rango de la Tarjeta**]**	El evento será relevante para un grupo definido de titulares de tarjeta.
Operator response time **[**Tiempo de respuesta del operador**]**	Si dentro del tiempo predeterminado el operador no contesta, esto será indicado en el sistema.
Save event in the Open Events file **[**Guardar evento en el archivo Eventos Abiertos**]**	Por predeterminación no marcado. Si marcado, este tipo de evento será guardado en el archivo **Open Events [**Eventos Abiertos**]** y exhibido en la pantalla **Maps [**Mapas**]**.

Indicación

Campo	**Descripción**
Presentation color **[**Color para presentación**]**	Usted puede atribuir un color específico al evento.
Sound **[**Sonido**]**	Usted puede atribuir un sonido específico al evento.
Popup Message **[**Mensaje emergente**]**	Un mensaje emergente que aparecerá en el visor del terminal en caso de ocurrencia de un evento.

Actividad automática

Envío de SMS: Durante un evento es posible enviar un mensaje SMS de indicación a un teléfono celular de una lista de abonados. Para más detalles, véase “SMS (solamente versión PRO)” en la página 16.

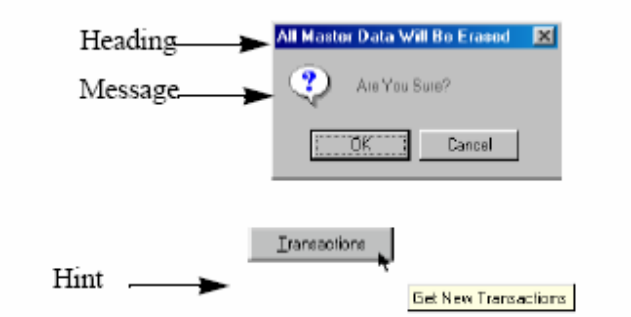
Instrucciones al operador

Permite escribir texto libre de instrucciones al operador del evento.

Capítulo 8 – Traducción de Mensajes

Falcon posibilita cambios en el lenguaje del interfaz a un idioma de destino seleccionado por el usuario. Este procedimiento es generalmente realizado por el distribuidor y también puede ser emprendido por el usuario sin dificultad. *Falcon* puede almacenar hasta tres distintos idiomas dentro del sistema. Uno en uso, y dos "a disposición". El proceso de la traducción es combinado, se hace dentro del software y usa una utilidad. Primero comience la traducción en el Falcon, después usando la utilidad según la explicación abajo.

Hay tres clases de anotaciones a ser traducidas:



En el Falcon usted debe:

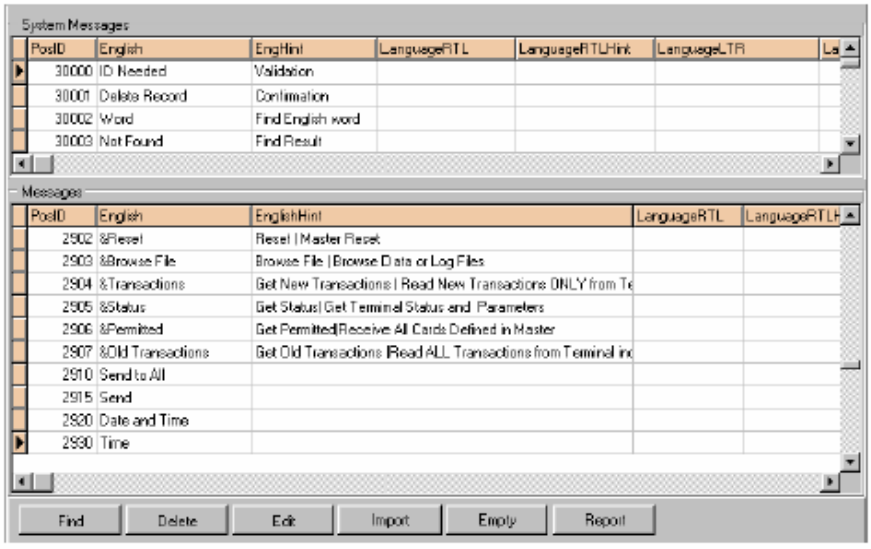
Paso 1. Vaya a **Setup | General Parameters | System | Localize** y asegúrese que el Idioma es **English**.

Paso 2. Retorne a **Setup** y seleccione el módulo **Message Translation [**Traducción de Mensajes**]**. La pantalla (véase abajo) es dividida en dos partes. La parte superior consiste en los actuales Mensajes del Sistema y la parte inferior consiste en Palabras y Títulos.

Paso 3. Para crear una lista de todos los textos en el sistema haga clic en **Import**. Esto llenará la tabla de mensajes (que está vacía por defecto) con el último texto en Inglés del actual EXE.

Nota: *Para asegurarse de que está importando el más actualizado texto, vaya a* **General Parameter |System** *y cambie* **Language [**Idioma**]** *para Inglés, y después* **Restart** *el programa*.

Su pantalla ahora aparecerá así:


System Messages
PosID English EngHint LanguageRTL LanguageRTLHint LanguageLTR
30000 ID Needed Validation
30001 Delete Record Confirmation
30002 Word Find English word
30003 Not Found Find Result
Messages
PosID English EnglishHint LanguageRTL
2902 &Reset Reset | Master Reset
2903 &Browse File Browse File | Browse Data or Log Files
2904 &Transactions Get New Transactions | Read New Transactions ONLY from Te
2905 &Status Get Status| Get Terminal Status and Parameters
2906 &Permitted Get Permitted|Receive All Cards Defined in Master
2907 &Old Transactions Get Old Transactions |Read ALL Transactions from Terminal in
2910 Send to All
2915 Send
2920 Date and Time
2930 Time
Find
Delete
Edit
Import
Empty
Report

Los títulos de las columnas tienen el siguiente significado:

English,	es designado para texto en Inglés
English Hint-	
Language RTL (caption text),	es designado para lenguas que se escriben de la
Language RTL Hint (hint text)	derecha para la izquierda (Hebreo/Árabe)
Language LTR (caption text),	es designado para lenguas que se escriben de la
Language LTR Hint (hint text)-	izquierda para la derecha

Paso 4. Traduzca el texto!

Paso 5. En **Setup | Calendar | Customize**, actualice el nombre de los días.

Paso 6. Salga del *Falcon* y active FaLang.exe.

Paso 7. Traduzca todos los archivos LU.

Paso 8. Salga de FaLang.

Paso 9. Una vez que todos los archivos necesarios (véase Lenguas Extranjeras, en la página 81) hayan sido traducidos usted puede enviarlos al departamento de soporte al usuario para preparar un nuevo conjunto localizado.

Para elegir un idioma particular que debe ser traducido:

1. Vaya a **Setup | General Parameters | System | Localize** y cambie el idioma para **Other** (si usted quiere que su Idioma reemplace las palabras: "**Other**", vaya a **Message Translation**, PosID 3576 para idiomas LTR y PosID 3574 para idiomas RTL, y anote el nombre de su Idioma).
2. Si requerido, cambia también la dirección.

Usando la Utilidad:

Paso 1. Algunas de las tablas de utilidad deben ser traducidas usándose el programa FaLang.exe. En su CD de instalación, vaya a **Utility** y copie FaLang.exe al PC donde el *Falcon* está instalado y actívelo. Usted tiene una lista de tablas de donde seleccionar, cada una contiene el texto en Inglés. Sobrescriba este texto con su texto apropiado.

Paso 2. Usted debe reempezar *Falcon* para que estos datos sean totalmente integrados. Para detalles adicionales, refiérase a "Apéndice B – Base de Datos".

Botones en la parte inferior de la pantalla:

El botón **Find** permite ubicar una palabra desde la localización actual. (Find Next) F3 ejecuta la búsqueda a partir de la última palabra. Una búsqueda parcial también está disponible (el inicio de una palabra).

El botón **Empty** limpia la parte inferior de la pantalla de todos los textos traducidos (así limpia todo el contenido del archivo de mensajes!).

El botón **Report** permite imprimir la lista de mensajes para fines de traducción.

RECOMENDACIÓN:

USTED DEBE REPASAR LAS PANTALLAS PARA ASEGURARSE QUE EL TEXTO ES ADECUADO Y QUE EL SIGNIFICADO ES EXACTO!

Capítulo 9 – Informes

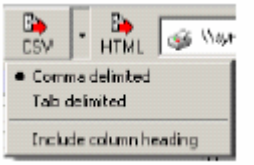
El *Falcon* consiste en los siguientes informes estándares que pueden ser seleccionados del menú **Informes** en el menú del *Falcon*:

- En línea
- Presencia/Ausencia (usted puede hacer clic en el icono **Presence Report** en lugar de eso)
- Transacciones (usted puede hacer clic en el icono **Report** en lugar de eso)
- Visitantes
- Eventos: Abrir, tiempo de respuesta, viejo
- Entradas
- Sistema (usted puede hacer clic en el icono **System** en lugar de eso)
- Grupo de Seguridad del Personal
- Lectoras por Grupo de Seguridad
- Zonas Horarias de Acceso a las Lectoras
- Repetidos: Tarjetas, Nombres, Identificaciones, Fotos
- Generador
- Informe Personalizado
- Adicionales: Fechas Prescritas, Tarjetas Emitidas, Personal Activo para el TimeLOG
- Incendio (menú **Emergencia**)

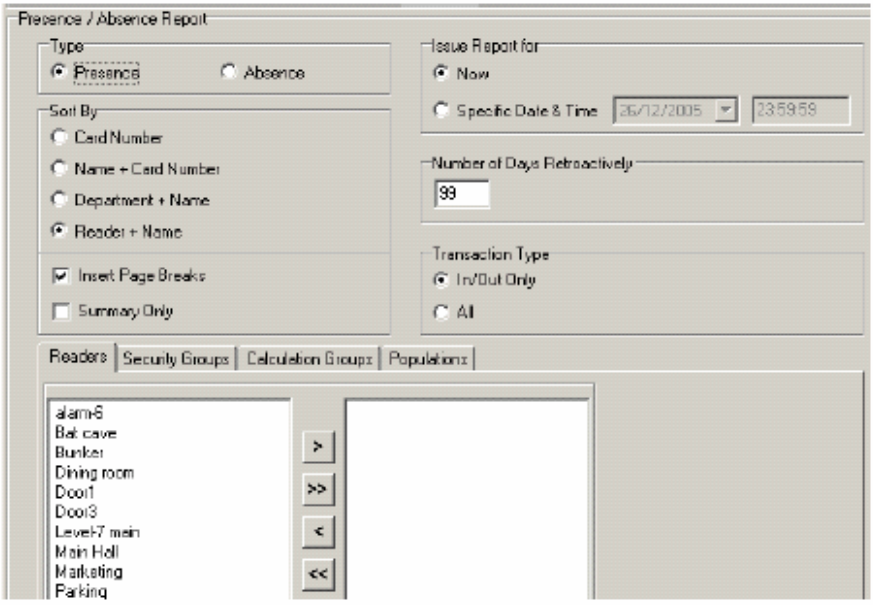
Estos informes pueden ser guardados en los formatos TXT, CSV (Excel) o HTML.

Avisos:

1. Haga clic con el botón derecho del ratón en una línea de informe en la pantalla del resultado para **Edit Employee [**Editar Empleado**]**.
2. En la misma pantalla usted puede definir los parámetros CSV:



9.1 Informe de Presencia / Ausencia



Elija **Presence** o **Absence** y después presione **Run**. Usted puede **Preview** o **Print** el informe. El informe **Presence** es producido a partir de la lista de personal activo (semejante al informe de incendio, véase Capítulo 13 – Localización, en la página 67). El informe de ausencia provee una lista de los empleados que están ausentes en el momento, según el orden especificado.

Si la casilla de verificación **Write Last Transaction into Personnel File [**Escribir la última Transacción en el Archivo Personal**]** es marcada, entonces el informe mostrará la última transacción correspondiente de los empleados (véase 3.3.2 Configuraciones del Sistema, en la página 10).

El informe puede ser producido para los días 0 (hoy) hasta 99 días retroactivamente.

9.2 Informe de Transacción

Este módulo permite emitir informes por transacciones según diversas categorías: fecha, tiempo, tarjeta, grupo de seguridad (presentación de todos los grupos de seguridad asignados), departamento, rangos de números de ID del empleado, nombre de los empleados, tipos de población (regular, visitante, guarda) y tipo de evento.

Es dividido en 3 fichas:

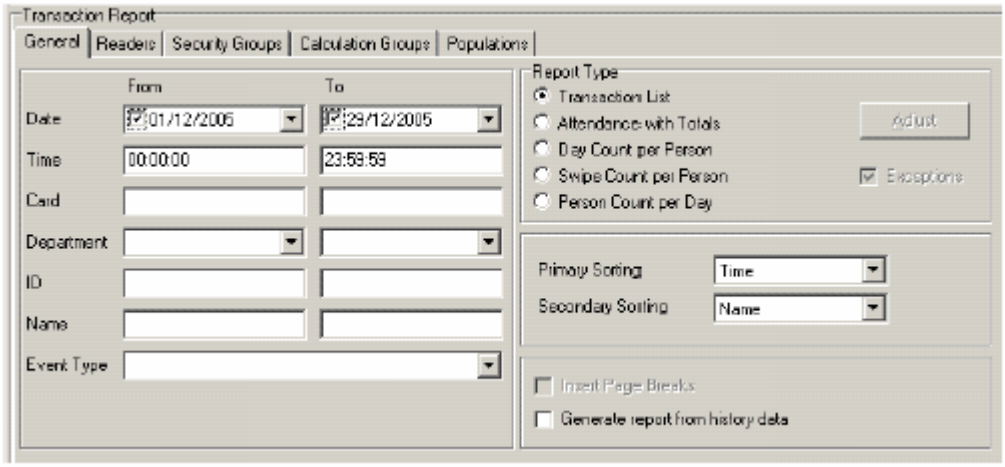
9.2.1 General

Este informe es dividido en 5 sub-informes.

Para todos estos tipos de informes los datos pueden ser producidos para un antiguo archivo de transacción. Todos los otros componentes del informe (así como: personal y terminales) serán tomados de la base de datos actual (para evitar incompatibilidad de formato de registro etc.). Para personal no más válido no aparecerá indicación de nombre. Marque la casilla de verificación Generate report from history data **[**Generar informe a partir de datos en la historia**]** para utilizar esta característica.

Transaction List [Lista de Transacciones**]**

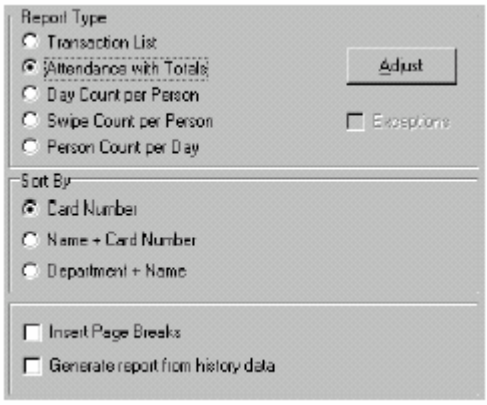
Este informe incluye eventos y transacciones no procesadas, y puede ser producido tanto para transacciones antiguas así como para actuales. Pueden ser clasificados por orden primaria y secundaria.



Los cuatro informes siguientes son resúmenes de diversas entradas-salidas y excluyen transacciones de evento:

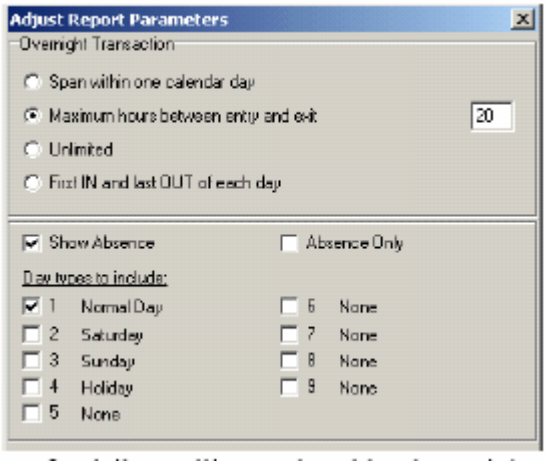
Attendance with Totals [Presencia con Totales**]**

Este informe presenta transacciones legales de entrada y salida, y no considera transacciones ilegales. Calcula totales por día, por empleado, por departamento y un total global.



Permite ordenar estas transacciones por: número de tarjeta, nombre del empleado+número de tarjeta, y nombre del departamento+nombre del empleado.

Presionando el botón **Adjust** se abre la siguiente pantalla:



Permite configurar las definiciones del usuario para un total diario, y permite determinar cuantos totales serán calculados. En la sección ausencia, se puede incluir datos de ausencia en el informe.

El botón de radio **First IN and last OUT of each day** permite la presentación de solamente la primera transacción legal para aquel día de trabajo y la última transacción del mismo día.

Nota: *A menos que usted marque los tipos de días a ser incluidos, los datos de ausencia no serán presentados (aunque la casilla de verificación esté marcada!).*

Day Count per Person [Número de Días por Persona**]**

Un informe estadístico que cuenta para cada persona el número de días en que se presentó durante un periodo específico.

Swipe Count per Person [Número de Fichadas por Persona**]**

Este informe cuenta el número válido de fichadas por un periodo especificado según los distintos tipos de transacción.

Este informe puede ser ordenado por: número de tarjeta, nombre del empleado+número de tarjeta, y departamento+nombre del empleado.

Nota: *Bajo* **Employee Details | Management | Expected Swipes**, *usted puede definir un límite de informe para aquel empleado.*

Si la casilla de verificación **Exceptions [**Excepciones**]** está marcada, solamente un total que no combine con los totales distintos del total indicado en el campo **Expected Swipes** será indicado.

Nota: *Asegúrese de que el total especificado bajo el campo* **Expected Swipes** *es para un periodo que combine con el periodo especificado en su informe!*

Person Count per Day [Número de Personas por Día**]**

Este informe cuenta cuantas personas se presentaron durante un día.

9.2.2 Lectora/Grupo de Seguridad/Grupo de Cálculo/Selección de Población

Por predeterminación todas las Lectoras/Grupos de Seguridad/Grupos de Cálculo/Población son incluidas en el informe. Si usted desea solamente información específica a ser incluida en el informe, márquela y haga clic en el símbolo >.

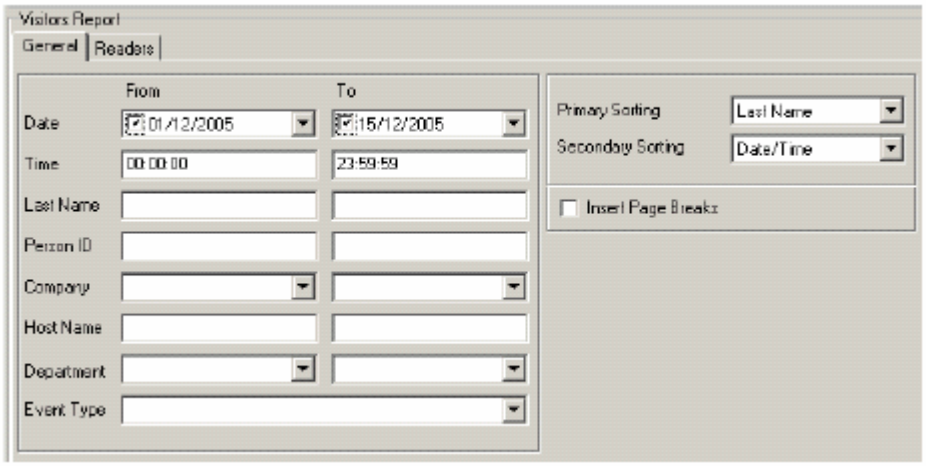
Para eliminar todos los ítems que fueron seleccionados, haga clic en el símbolo <<.

Para eliminar un ítem específico, selecciónelo en la columna de la derecha y haga clic en el símbolo <.

Haga clic en **Run**; la información relevante aparecerá en la pantalla **Transaction report [**Informe de Transacción**]**.

Nota: *Los parámetros del informe: Fecha, tiempo y tarjeta son procesados de manera más rápida que grupo de seguridad, departamento, ID y nombre, que irán a bajar la velocidad de producción del informe, si seleccionados.*

9.3 Visitantes



Este módulo permite producir informes por transacciones de visitante. Permite producir un informe según distintas categorías de rango: Fecha, Hora, Apellido, ID de la Persona, Compañía, Nombre del Anfitrión, Departamento, Tipos de Evento (regular, visitante, guarda).

Es dividido en 2 fichas:

9.3.1 General

El procedimiento para producir un informe es como sigue:

Paso 1. Haga clic en **Reports** en el menú principal, y después en **Visitors**.

Paso 2. Para crear un informe defina los parámetros mencionados arriba y el orden preferido.

Paso 3. Después de entrar la información en los campos, haga clic en **Run**.

9.3.2 Lectoras

Por predeterminación todas las lectoras son incluidas en el informe. Si usted quiere incluir solamente lectoras específicas, márquelas y haga clic en el símbolo >.

Para remover todas las lectoras que fueron seleccionadas, haga clic en el símbolo <<.

Para remover una unidad específica, selecciónela en la columna de la derecha y haga clic en el símbolo <.

9.4 Eventos

Hay 3 distintos informes de eventos:

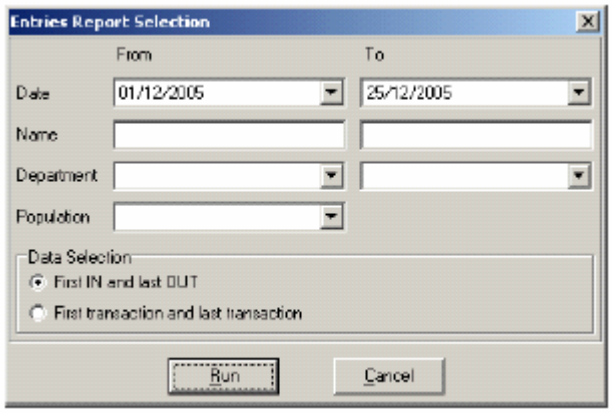
Eventos Abiertos- Un informe del rango horario de eventos que todavía no fueron atendidos.

Tiempo de Respuesta- Indica la frecuencia de la reacción del operador a los eventos. (El intervalo de tiempo entre el comienzo del evento y la respuesta del operador).

Eventos pasados- Un informe del rango horario de eventos concluidos.

9.5 Entradas

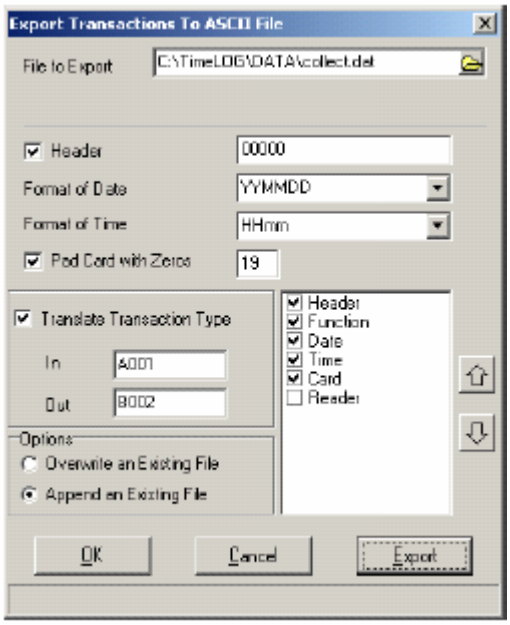
Este informe presenta todas las transacciones legales y es designado para exportar datos al TimeLOG. Cada entrada y salida es presentada en un registro separado. El informe puede ser ordenado por nombre del empleado, departamento y población.



La sección de Selección de Datos ofrece dos posibilidades:

- Presenta la primera Entrada y la última Salida de un empleado para el periodo especificado.
- Presenta la primera transacción y la última transacción de un empleado para el periodo especificado.

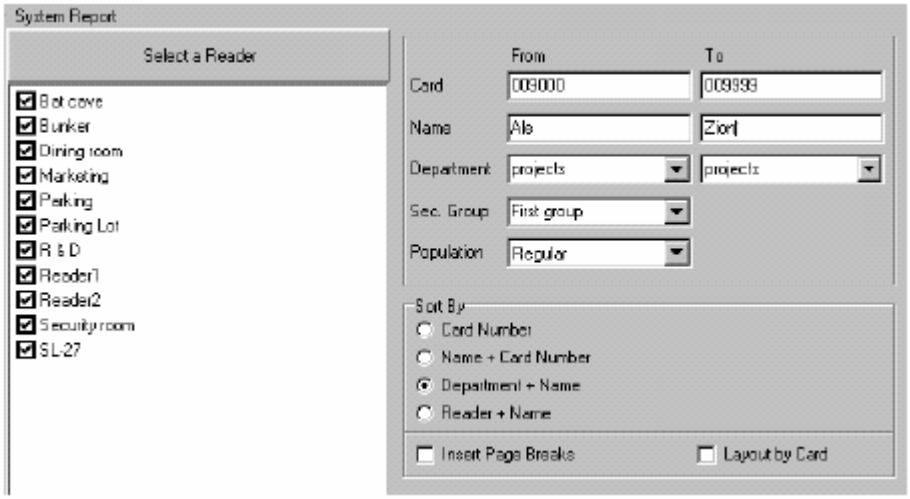
Este informe puede ser exportado a un archivo ASCII según las especificaciones del usuario. Véase la pantalla **Export transaction [**Transacción de Exportación**]** abajo:



Este informe filtra las transacciones de control de acceso para fines de control de presencia. Son mostrados los componentes potenciales del archivo. Usted puede organizar la lista en orden de prioridad y debe conferir los ítems a ser incluidos en su archivo de exportación. En la pantalla arriba está esbozado un archivo de exportación al TimeLOG.

9.6 Sistema

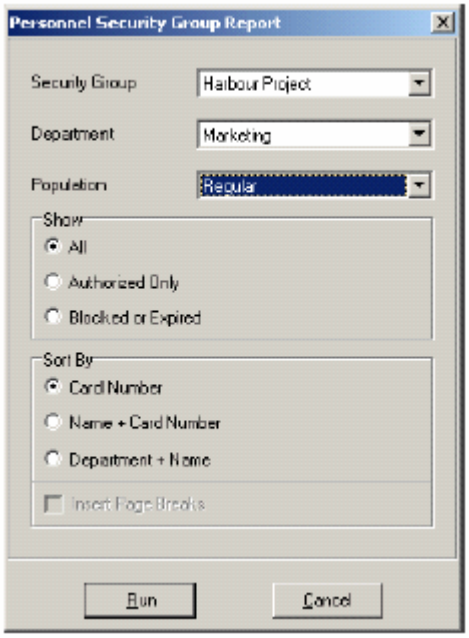
El informe del sistema detalla los individuos que tienen acceso a cada puerta y esboza sus restricciones de acceso. Para generar un informe del Sistema:
Abra **System Report**, seleccione los terminales relevantes y haga clic en **Go**.



Una filtración ampliada por rangos de tarjeta/nombre/departamento y varias formas de ordenación facilita la gerencia del acceso del empleado.

Es posible imprimir, ver una presentación preliminar o exportar este informe a HTML.

9.7 Grupo de Seguridad del Personal



Enumera todas las personas que pertenecen a un grupo.

9.8 Lectoras por Grupo de Seguridad

Un informe fijo que presenta información al respecto de la asignación del grupo de seguridad.

9.9 Zonas Horarias de Acceso a las Lectoras

Un informe fijo que presenta información al respecto de la asignación del grupo de seguridad, incluyendo datos de la zona horaria (permite comparación entre zonas horarias y grupos de seguridad).

9.10 Repetidos

9.10.1 Tarjetas Repetidas

Todas las tarjetas de empleados que fueron indicadas más de una vez en el archivo **Personnel**.

Nota: *Por predeterminación este informe debe estar vacío! Si no, esto significa que un error debe ser rectificado!*

9.10.2 Nombres Repetidos

Todos los nombres de empleados que fueron indicados más de una vez en el archivo **Personnel**.

9.10.3 IDs Repetidas

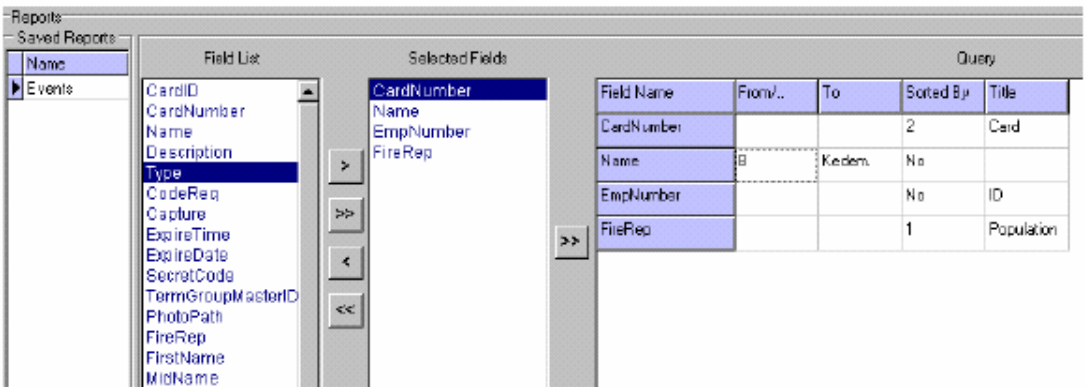
Todos los números de ID de empleados que están indicados más de una vez en el archivo **Personnel**.

9.10.4 Fotos Repetidas

Todas las fotos de empleados que fueron indicadas más de una vez en el archivo **Personnel**.

9.11 Generador

Existen diversas maneras de imprimir informes de transacciones de secciones-cruzadas por empleado o por un grupo de empleados. Estos informes se generan de plantillas incorporadas que pueden ser creadas/generadas por el usuario. Cuando el usuario guarda un informe personalizado un sub-menú será agregado al menú **Customized report**.



Creando un informe

Paso 1. En la pantalla **Report Generator [**Generador de Informe**]** haga clic en el botón **Select Table [**Seleccionar Tabla**]** y seleccione una tabla Paradox.

Paso 2. Haga clic en el botón >> para colocar todos los campos en el Informe, o seleccione un campo de la **Field List [**Lista de Campos**]** y haga clic en el botón >.

Paso 3. Entre los rangos relevantes para cada campo, y defina la prioridad de orden, haciendo doble clic en el campo relevante (Una selección de prioridad puede ser anulada haciendo doble clic una segunda vez).

Paso 4. Haga clic en el botón **Go** para crear un informe y en el botón **Preview** para visualizar el informe en la pantalla.

Paso 5. Para imprimir el informe, haga clic en el botón **Print**.

Creando una plantilla de informe

Cuando guardadas, estas nuevas plantillas de informe son automáticamente almacenadas bajo **Reports | Customized Report** para uso futuro.

9.12 Informe Personalizado

Todos los informes que fueron generados a través del generador de informes son almacenados aquí para uso futuro.

9.13 Adicionales

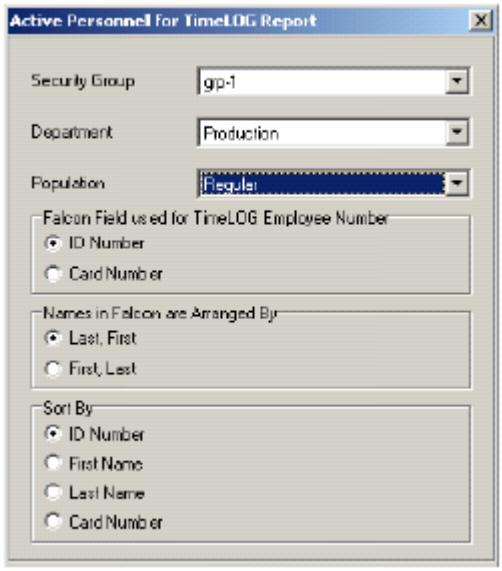
9.13.1 Fecha Prescrita

Una lista de todas las tarjetas que han caducado.

9.13.2 Tarjetas Emitidas

Una lista de las últimas fechas de emisión de tarjetas que fueron impresas (botón **Print card** solamente para la versión PRO) durante un periodo especificado.

9.13.3 Personal Activo para TimeLOG



Este informe es designado para exportar la base de datos activa de empleados del *Falcon* al TimeLOG, filtrados o no, según la preferencia del usuario. Puede también ser ordenado por: ID, Nombre/Apellido y tarjeta.

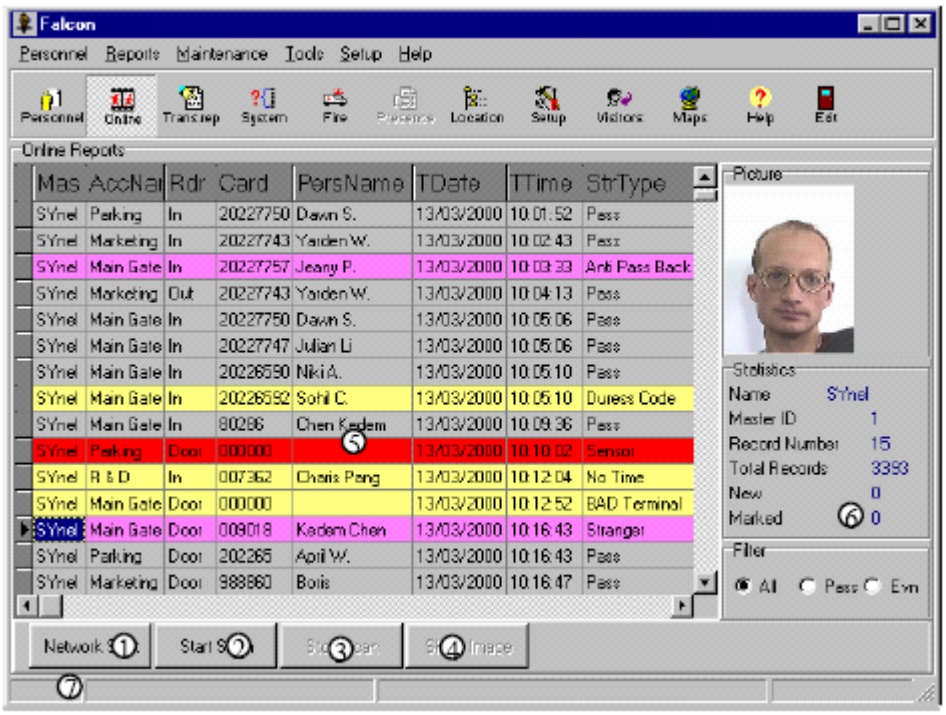
Dos secciones determinan donde insertar el campo de origen de los datos en el campo de destinación del TimeLOG:

- **Falcon Field used for TimeLOG Employee Number**: si presentar el campo **ID Number** o los campos de origen **Card Number** bajo el campo de destinación **Employee Number** en el TimeLOG.
- Informar al TimeLOG de la orden del nombre completo del empleado: qué viene primero: el apellido o el nombre (en el Falcon ambos están bajo un campo, en el TimeLOG están bajo dos campos separados).

Capítulo 10 – Trabajando en Línea

Soportado solamente por un terminal local o por comunicación TCP/IP Master o terminales SY-400 (no COM-II-PRO o MÓDEM - para estos terminales la frecuencia de la colección de datos puede ser definida en **Options | Automatic scheduling | Collect data**). Este módulo presenta una tabla en línea de datos actuales como recogidos de los terminales.

La foto en el lado izquierdo de la pantalla es de la transacción del último titular de la tarjeta. A medida que son obtenidos datos de las transacciones las fotos cambian en conformidad, y las estadísticas son actualizadas. El estado activo/inactivo del vínculo de comunicación es exhibido. Hay una opción de filtración para exhibir transacciones de todo/no evento/evento.
Además, haciendo clic con el botón derecho del ratón en una fila permite que el usuario edite la pantalla de los detalles del empleado.



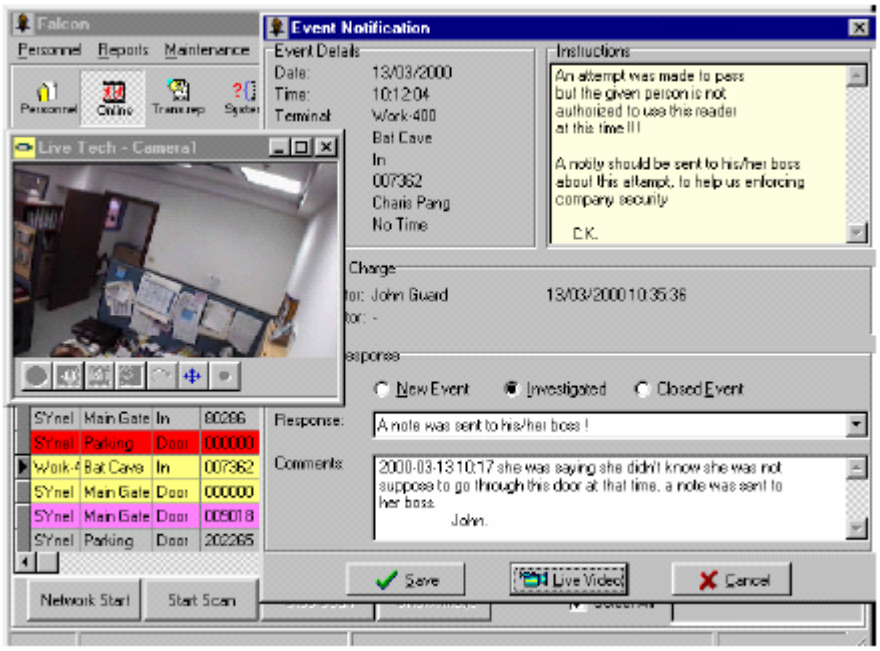
	Nombre del campo	Descripción
1	Auto Refresh	Empieza a actualizar la pantalla, pasa a la última línea en una frecuencia predeterminada (véase 3.4.1. Opciones, en la página 12). No hay comunicación con los terminales, y esta actividad es designada para mostrar los nuevos datos que fueron recogidos por otra estación de trabajo (PC de colecta de datos) u otro software (Servidor-SY).
2	Start Scan	Empieza la colecta de datos (consulta) de todos los terminales activos.
3	Stop Scan	Termina **Start Scan** o **Auto Refresh.**
4	Show image	Exhibe detalles y una imagen de tamaño grande de la última transacción colectada, permitiendo filtrado por lectora. Una presentación de video (solamente en la versión PRO) puede emerger para que el operador pueda compararla con la imagen guardada en la base de datos. Esta característica es habilitada solamente cuando **Auto Refresh** o **Start-scan** están activos.
5		Haciendo doble-clic en esta pantalla, aparece la pantalla **Event notification** (véase Cap. 7 - Eventos, en la página 47 y véase 10.1. Administración de Eventos en Línea, en la página 61).

	Field name	Description	
6	Statistics displayed	Nombre	El nombre de la unidad del terminal que envía sus datos (Definida en la Lista de Terminales).
		Master ID	La ID de la unidad del terminal (definida en la Lista de Terminales).
		Número del registro	El registro de datos actualmente seleccionado.
		Número total	El número total de registros de datos en línea.
7		Indicación de una actividad en progreso.	

Pantalla Mostrar Imagen

10.1 Administración de Eventos en Línea

La administración de eventos es realizada a través de la pantalla **Event notification [**Notificación de Evento**]** en la carpeta **Online [**En Línea**]**. El control de eventos es implementado rastreándose la ocurrencia del evento y rápidamente tomando medidas (operador). El estado del evento, comentarios e instrucciones pueden ser actualizados en línea.



Nota: *Para acelerar el procedimiento, utilice las teclas* **F7/F8** *que: marcarán un evento como* **Investigated/Closed**, *guarde y salga de la pantalla.*

10.2 Borrar la tabla en línea

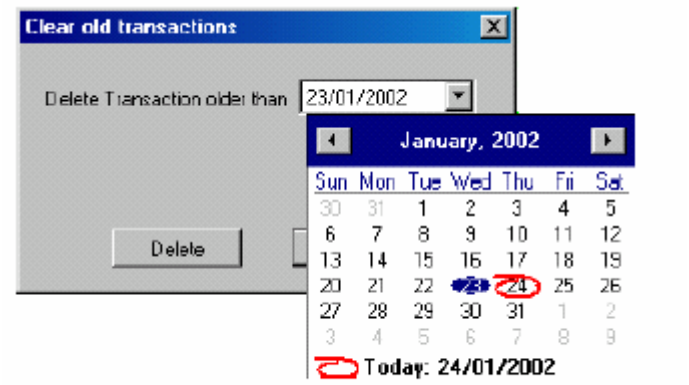
Para borrar datos de la base de datos en línea:

Paso 1. Haga clic en **Maintenance** en el menú principal y después en **Clear transactions**.

Paso 2. Seleccione el campo **Date**, después seleccione la fecha por la cual suprimir todas las transacciones de la presentación de la Tabla en Línea. Estas transacciones son suprimidas PERMANENTEMENTE del archivo **Transaction [**Transacción**]**.

Se recomienda realizar copia de seguridad antes de borrar datos de la base de datos en línea.

Nota: *Si hay muchas transacciones en la tabla (20,000 o más), podría tomar algunos minutos para borrar los datos, por favor sea paciente.*



Capítulo 11 - Visitantes

Visitantes son parte integral de la actividad diaria de una empresa. Falcon tiene la capacidad de proveer a cualquier número de visitantes tarjetas de acceso fácilmente supervisadas y administradas.

11.1 Creando tarjetas vía Personal

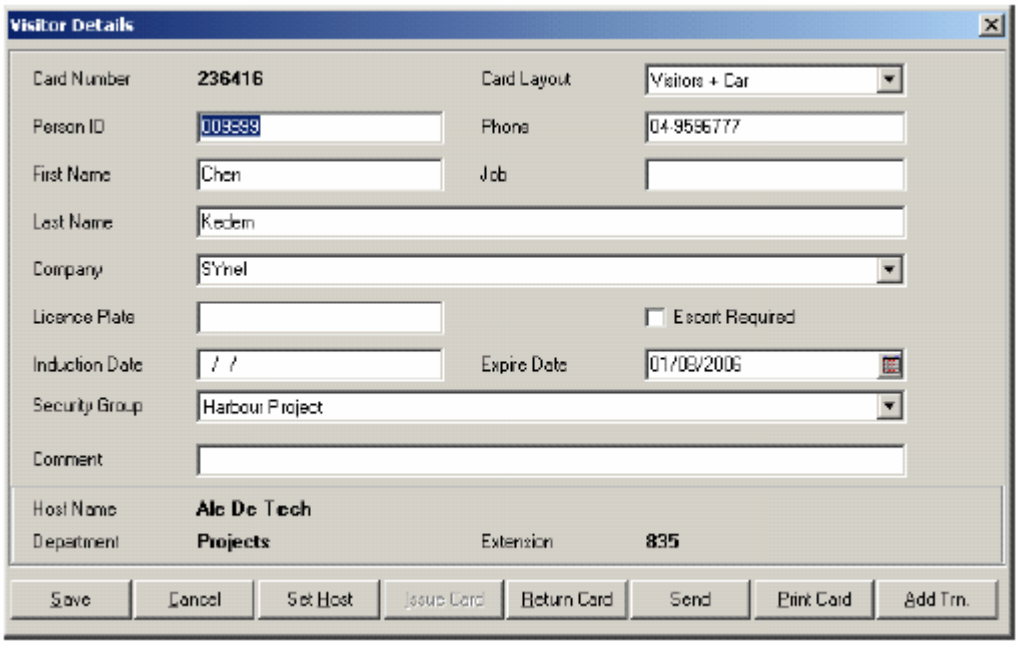
Bajo **Personnel** todas las tarjetas son establecidas. Para visitantes, que es un caso único de tarjetas, usted debe primero crear aquí una nueva línea, que consiste en **Card Number, Name** y seleccionar **Visitor** como el **Population Type**.

11.2 Manejo de visitantes

Añadir un Nuevo visitante

Paso 1. Haga clic en **Visitor**; la pantalla **Visitor List [**Lista de **Visitantes]** aparece.

Paso 2. Haga clic en **New**; la pantalla **Visitor Details [**Detalles de Visitantes**]** es exhibida (abajo). Anote los detalles y asigne el/ella a un **Security Group**.



Paso 3. Haga clic en **Set Host** para atribuir un anfitrión a su visitante (de la pantalla **Personnel**). El anfitrión es un empleado responsable de manejar asuntos de visitantes dentro de la organización.

Paso 4. Para emitir una tarjeta usted puede hacer clic en el botón **Issue Card** y anotar el número definido en **Personnel**, o utilizar una lectora emuladora de teclado para leer el número de la propia tarjeta.

Paso 5. Haga clic en **Save**; los nuevos detalles son exhibidos en la pantalla **Visitors List**.

Paso 6. Elija también una disposición de tarjeta. Para crear un nuevo croquis de tarjeta, véase el párrafo 3.4.3: "Editar Disposición de Tarjeta (solamente en la versión PRO)", en la página 18 (usted puede también imprimir la tarjeta usando el botón **Print Card**).

Si requerido, usted puede añadir manualmente una transacción a este visitante. Esto se puede hacer después de la asignación de la tarjeta, para marcar el horario en el cual ha sido asignada la tarjeta específica al visitante.

Retornar la Tarjeta

Para despedir un visitante de las facilidades de su organización, haga una de las opciones:

- En la misma pantalla haga clic en el botón **Return Card**.
- En la pantalla principal de Visitantes, haga clic en **Return Card**, anote el número de la tarjeta y haga clic en **Yes**.

Ahora el visitante no tiene más permisión de acceso a sus oficinas. Sus entradas y salidas han sido registradas en el sistema.

Las transacciones del visitante son registradas bajo el nombre del visitante. Para más información refiérase al capítulo **Informes**, párrafo 9.3: "Visitantes", en la página 55.

Nota: *Mientras emitiendo/retornando la tarjeta, el visitante es automáticamente transmitido a todos los terminales Master actualmente/previamente autorizados.*

Nota: *La opción* FIND *activa una búsqueda incremental.*

Nota: *Múltiples filas de visitantes pueden ser resaltadas (sosteniendo Shift+Arrow) y presionando Ctrl+Delete el usuario puede suprimir todos los visitantes marcados.*

Nota: *Usted no podrá suprimir un visitante a menos que reciba su tarjeta y haga clic en el botón* **Return Card** *respectivamente.*

Capítulo 12 - Manutención

Este módulo consiste en ocho ítems de menú que le permiten realizar una variedad de actividades estándares de manutención.

Collect Data **[**Colectar Datos**]** – Colecta nuevas transacciones de todos los terminales activos.

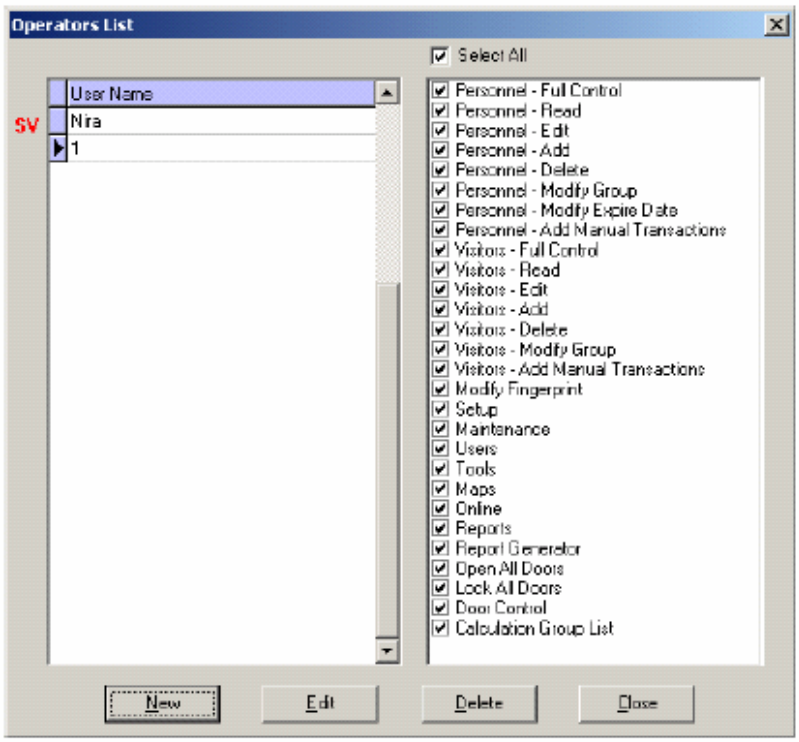
Send All Data **[**Enviar Todos los Datos**]** - Reprograma todos los terminales activos para reflectar cambios en el sistema.

Send Updates **[**Enviar Actualizaciones**]** – Envía las recientes actualizaciones y nuevas plantillas de huellas digitales de la lista autorizada a todos los terminales Master o SY-400.

Users **[**Usuarios**]** – Permite definir el nivel de seguridad de un operador del sistema limitando el acceso a los módulos del *Falcon* según el caso. El acceso a un modulo es permitido señalándose la casilla de verificación. Observe la variedad de opciones de edición en las pantallas **Personnel [**Personal**]** y **Visitor [**Visitante**]** (Añadir, Eliminar, Alterar Grupo, etc.) Otro medio de restricción del operador es el nivel de permiso que es determinado al definirse un nuevo usuario o al editar un usuario existente. Aquí usted debe anotar el nombre de usuario del operador del sistema, la contraseña y el nivel de permiso. El valor máximo del nivel de permiso es 9. Actualmente ese medio de nivelar es implementado apenas para grupos de seguridad. Esto significa que un usuario puede asignarse a un grupo de seguridad solamente si su nivel del permiso es más bajo o igual al suyo. Para más informaciones, véase el párrafo 5.5 Definir un Grupo de Seguridad, en la página 43.

Una vez que un operador de sistema con acceso a **Users [**Usuarios**]** es definido, una contraseña debe ser insertada para dar inicio al *Falcon.*

Preste atención: Un supervisor debe ser definido según esta explicación. **Cerciórese de que esté definido por lo menos un supervisor en cualquier momento dado. ¡De lo contrario, nuevos usuarios no pueden ser añadidos!**



Backup **[**Copia de Seguridad**]** – Guarda un archivo de base de datos en formato ZIP para futura utilización. Para crear una copia de seguridad en formato ZIP, haga clic en **Backup**, de un nombre al nuevo archivo y haga clic en **Save [**Guardar**].**

Nota: *Falcon.ini también tiene copia de seguridad (el soporte técnico puede detectar definición de parámetro que originaron problemas en este archivo). Como precaución, este archivo no se abre durante el procedimiento de restauración .*

Restore **[**Restaurar**]** –El directorio restaurado será guardado bajo el mismo nombre y bajo el mismo directorio (sin la extensión ZIP). La restauración engloba dos funciones:

1. Files Restore **[**Restauración de Archivos**]** – Recupera un archivo de base de datos en el formato ZIP y lo guarda como tal en el directorio. Después de recuperar el archivo de base de datos, usted puede volver a cargarlo al sistema como un archivo operacional de base de datos. Para hacer esto, elija **Alias to Restore** (bajo **Restore**).
2. Alias to Restore **[**Alias para Restaurar**]** – Permite cambio de referencia de la base de datos para fines de restauración, sin sustituir los archivos. Haga clic en **Alias to Restore**; el directorio del archivo se abre. Elija el directorio requerido. *Falcon* se cerrará automáticamente a fin de actualizar los cambios de definición. Entonces, reinicie el programa

Nota: *No recolecte datos mientras trabaja con datos restaurados .*
Vuelva a su carpeta actualmente usada solamente después que los datos restaurados hayan sido manejados.

Nota: *Antes de la operación de copia de seguridad y restauración, en una específica estación de trabajo, el Falcon informará a todas las otras estaciones de trabajo que sus bases de datos serán encerradas durante 90 segundos .*
*Asegúrese que el campo **Event Signalling Frequency [**Frecuencia de Señalización de Evento**]** (bajo **Tools| Options| Online**) tiene un valor superior a cero!*

ReIndex **[**Reindexar**]** – Reorganiza la base de datos cuando ocurre corrupción de un archivo en los archivos de índice. Para más información, véase el párrafo ReIndex.exe, en la página 83 .

Nota: *Durante la instalación es creado un acceso directo (**Start | Programs | Falcon**). Este activa **Reindex /Repair** para ayudar a los clientes con el procedimiento de reparación .*

Clear transaction **[**Borrar Transacción**]** – Omite todos los tipos de transacción (transacción, eventos en abierto/cerrados) en una base diaria (véase el Capítulo 10 – Trabajando en Línea, en la página 60)

Synchronize fingerprint **[**Sincronizar Huellas Digitales**]** – Para más información refiérase al párrafo 15.3 Sincronizando Plantillas, en la página 74.

Capítulo 13 – Localización

Permite actualizar los datos del terminal, haciendo que la manutención del sistema sea más rápida y más simple. Para actualizar y ver los datos del terminal sin entrar en la pantalla **Setup**:

Paso 1. Entrar en la pantalla **Location**. Hacer clic en el botón **Location**.

Paso 2. Señalar el terminal específico y hacer clic en el botón derecho del ratón. Hacer clic en **Edit** en el menú emergente. La relevante pantalla **Terminal Setup** aparecerá.

Completar los varios campos en las cuatro fichas y continuar como indicado en la carpeta **Setup**.

Un clic en el botón derecho del ratón en un terminal/lectora abre un menú de contenido sensitivo permitiendo ver un video al vivo (solamente en la versión PRO) y el control de la puerta, como sigue:

Properties-	Abre la pantalla de configuración del terminal/lectora donde se puede cambiar las definiciones de la cámara+las definiciones del control de acceso.
CCTV Live View-	Permite activar la cámara conectada a este terminal/lectora.
CCTV Disconnect Site-	Desconecta la conexión de la cámara.
Open Door-	Permite mantener la puerta constantemente abierta.
Lock Door-	Permite mantener la puerta constantemente cerrada.
Door to Normal-	Permite revertir la puerta a su modo predeterminado de transmisión.

13.1 Emergencia

13.1.1 Producir un Informe de Incendio (emergencia)

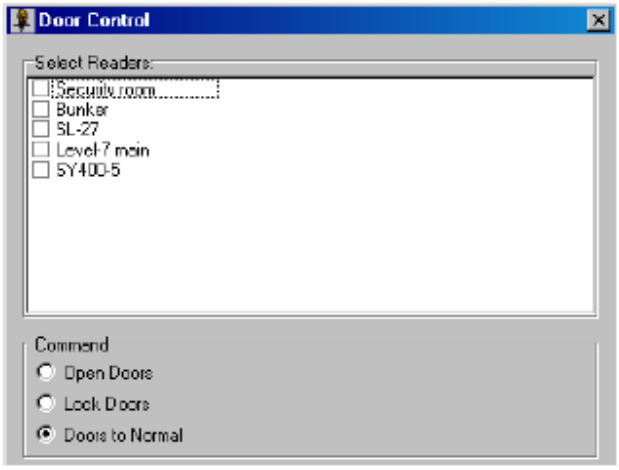
Exhibe en tiempo real los datos de frecuencia de los empleados y visitantes que están dentro de las instalaciones. Semejante al informe **Presence** pero antes de la emisión de este informe el software recoge datos de todos los terminales activos.

Nota: *Las siguientes definiciones serán determinadas a través del informe **Presence** (no pueden ser definidas bajo las configuraciones del informe Incendio):*
Ordenar Por
Insertar Salto de Página
Número de Días Retroactivamente
Tipo de Transacción

13.1.2 Control de la Puerta

Permite la administración de todos los puntos controlados de la lectora de entrada en una emergencia: abrir/cerrar todas las puertas, revertir las puertas al normal o controlar cada puerta manualmente (Control de la puerta). Además, los cambios en el modo de la puerta son representados gráficamente (LED rojo/verde) bajo **Location [**Localización**]**.

Bajo **Door Control [**Control de la Puerta**]** se puede cambiar el modo de transmisión por lectora:



Open Doors - Permite mantener todas las puertas constantemente abiertas.
Lock Doors - Permite mantener todas las puertas constantemente cerradas.
Doors to Normal - Permite revertir todas las puertas a su modo predeterminado de transmisión.

Nota: *Las configuraciones de emergencia suplantan la definición predeterminada de supervisión de la lectora de la puerta.*

Capítulo 14 – Mapas

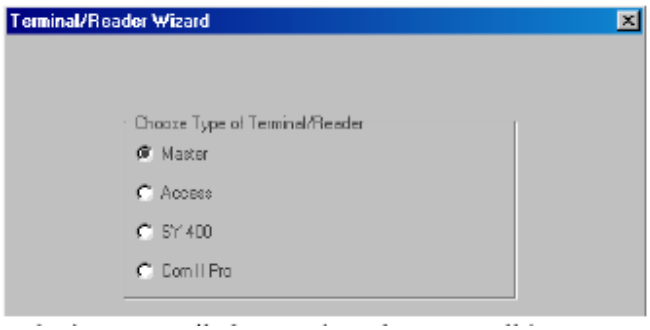
La característica Mapas es proyectada para exhibir visualmente notificaciones de eventos en un mapa de dispositivos de hardware de control de acceso de la organización. Al entrar a esta pantalla *Falcon* sincroniza el estatus del regulador y de la lectora en el módulo Mapa. El operador puede, entonces, detectar en línea la localización exacta del evento. Los mapas pueden ser presentados jerárquicamente y permiten aumentar (zoom) áreas menores. Los mapas pueden ser editados en la pantalla designada **Edit Maps [**Editar Mapas**]**. La pantalla **View Map [**Visualizar Mapa**]** permite a los operadores ubicar y manejar eventos en el sitio.

Como precaución, si más de 100 eventos siguen abiertos (no tratados), los últimos 100 eventos actualizados permanecen en abierto y los otros son almacenados en la carpeta de eventos cerrados clasificados como cerrados automáticamente. Simultáneamente, un mensaje de alerta aparece notificando al operador que 100 eventos no fueron tratados.

Edit site **[**Editar Sitio**]**

Paso 1. Haga clic en el menú descendente **Tools [**Herramientas**]** y después en **Edit site.** La pantalla **Edit site** aparece exhibiendo todos los dispositivos de acceso actualmente instalados.

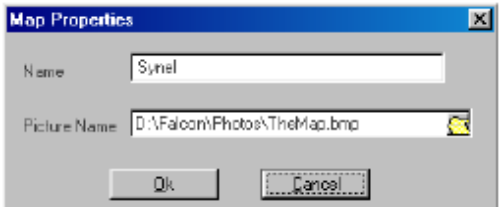
Paso 2. Al hacer clic con el botón derecho del ratón, usted puede añadir un nuevo terminal / lectora o cualquier otro nuevo dispositivo de hardware.



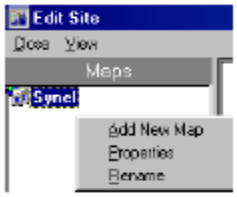
Paso 3. Por favor observe que los íconos están amontonados, así que para ver todos los íconos usted debe arrastrarlos y colocarlos sobre el mapa.

Nota: *Falcon no incluye una opción para dibujar mapas o para escanear un mapa; por lo tanto los mapas deben ser dibujados con las herramientas estándares de Windows e importados como un archivo JPG o BMP*.

Paso 4. Para agregar un dibujo de fondo de sus premisas, haga clic en el icono **Properties [**Propiedades**]** y hojee para encontrar el archivo BMP o JPG:



Paso 5. Para crear un nuevo mapa, coloque el cursor en el árbol del mapa y haga clic con el botón derecho del ratón. Haga clic en **Add new map [**Agregar nuevo mapa**]**:



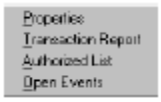
De un nombre al mapa. Usted puede agregar un sub-mapa bajo el mapa existente. Usted puede también arrastrar y colocar iconos de mapa a mapa.

Paso 6. El cambio de la posición de terminales/lectoras es hecho arrastrándose y colocándose el dispositivo relevante en el mapa requerido.

View site (Main tool bar) **[**Visualizar sitio (Barra principal de herramientas)**]**

El *Falcon* puede exhibir en línea indicación y ubicación de evento (Automáticamente actualizados). En el caso, obvio, que los datos hayan sido colectados.

- Permite visualizar el mapa de sus premisas y los eventos actuales, simultáneamente.
- Cada Evento es resaltado cronológicamente y el terminal equivalente es enmarcado en rojo.
- Los dispositivos que no están activos (la casilla de verificación **Active**, en la ficha **General** en la pantalla **Terminal setup** no está señalada) son marcados por una línea roja diagonal. Si hay un evento que pertenece a un terminal que no aparece en el momento, el icono relevante del mapa será enmarcado en rojo.
- Hacer doble clic en un mapa induce a la presentación del mapa.
- Hacer doble clic en un terminal induce a resaltar el evento en abierto de más alto nivel.
- Al hacer clic con el botón derecho del ratón en un icono de controlador, aparecerá la pantalla **Terminal setup**. Esto permite ajustar los parámetros de configuración.
- Al hacer clic con el botón derecho del ratón en un icono de lectora, aparece el contenido de este menú:



Properties **[**Propiedades**]** – La pantalla de configuración de la lectora permitiendo el ajuste de los parámetros de configuración
Transaction report **[**Informe de transacción**]** – Permite presentar una consulta (véase Capítulo 7 - Eventos, en la página 47).
Authorized list **[**Lista autorizada**]** – Una lista de todas las tarjetas aprobadas para la lectora específica.
Open event **[**Evento en abierto**]** – Permite presentar una consulta, véase Capítulo 7 - Eventos, en la página 47.

Capítulo 15 – Huellas Digitales

Nota: *Firmwares más antiguos respaldan la unidad MV-1200 con ID de 6 dígitos. Véase la tabla abajo para variaciones de específicos firmwares*:

Versión Firmware	Tipo de Unidad de Huella Digital	No. de dígitos de ID
5.115, 6.101 +	MV1200	7-8
6.200	MV1200	9-10
8.032x	MV1200	10
8.033x	FPU-S	10

Los conceptos biométricos básicos son:

Inscripción

Explorando una huella digital, determinando la calidad de la exploración y almacenando una buena plantilla como referencia, la inscripción es confirmada y la calidad de los datos explorados es resaltada. La calidad de la exploración es un subproducto de la condición de la piel: piel seca puede contribuir para una imagen no fiable. Una cantidad normal de humedad en la piel hace sobresalir los surcos y valles de la huella digital al sensor. Muy poca humedad hace la imagen "ruidosa" y causa rechazo de la imagen por parte de la unidad de inscripción durante el proceso. Humedecer ligeramente el dedo realzará el contraste de la impresión y proporcionará una verificación más confiable. Una sensibilidad creciente del sensor de silicio puede reducir dramáticamente estos problemas.

Identificación

No requiere una tarjeta/código. Las plantillas de Huellas Digitales son almacenadas en la memoria del terminal. Siempre que un empleado coloca su dedo en el sensor, la unidad Fingerprint **[**Huellas Digitales**]** (FP) explora todas las plantillas existentes hasta encontrar la que corresponde y confirma/rechaza.

Verificación

Requiere una tarjeta/código. La plantilla es almacenada con referencia a una tarjeta/código. Las tarjetas/códigos y plantillas son almacenados. Cuando un empleado ficha su tarjeta/introduce este código, la unidad verifica si el número de tarjeta/código existe; si es positivo, verifica también la plantilla asignada a este número.

Todas las unidades pueden realizar inscripción a través de su Terminal, mientras que cada unidad ofrece características y rangos diferentes como se ve a seguir:

Calidad

El grado de Calidad está basado en que bien está definido el patrón de los surcos dentro de la imagen de la huella digital que fue inscrita. La calidad mide cómo claramente la unidad reflejó la huella digital. Inscripción de baja calidad puede dar lugar a un índice elevado de rechazamiento falso haciendo difícil para el usuario verificar la confiabilidad. El grado es de 0 a 100. 100 es la mejor calidad (obtenida raramente) y 0 la peor. Los grados de calidad de 40 y más altos actúan bien con el algoritmo de verificación que compensa fácilmente las diferencias en la huella digital.

Contenido

El grado de Contenido está basado en la cantidad de información usable que la unidad observa en la huella digital. Las plantillas que son caracterizadas por bajo grado de contenido pueden dar lugar a índices elevados de falsa aceptación.

El grado se extiende de 0 a 100. 100 es el contenido máximo y 0 el valor mínimo.

Grados de contenido de 20 o más altos actúan bien con el dispositivo de inscripción. En este rango el algoritmo tiene suficiente información para distinguir entre diferentes huellas digitales con un alto grado de precisión. Plantillas con grados de contenido superiores a 20 no cambian en termos de índices de errores.

	No. de Plantillas en el Terminal	**Plantillas por empleado***	**Guardar en tarjeta Mifare ****	**Inscripción en PC**
Verificación	4000	10	+	PRintX
Identificación	200	10	-	PRintX
FPU-S	1000-9000	1	+	PRintX o lectora USB

* Inscripción en PC permite hasta diez plantillas por empleado (dos plantillas en la versión Express).

Inscripción en terminal permite hasta dos plantillas por empleado.

** Al guardar una plantilla en una tarjeta Mifare, solamente una plantilla por persona puede ser usada.

15.1 Hardware

El hardware requerido es como sigue:

Terminales Compatibles

SY-400 o SY-780/A

Unidades de Lectura Compatibles

- PRintX/H (serial) o FP-S200/FP-S300 (USB)
- Lectora/escritora Mifare (Posibilidad de guardar plantilla en tarjeta)

15.1.1 Definiciones de SY-400

Terminales

Para instrucciones de configuración véase el párrafo 5.3.3: "Definir un Terminal SY-400 ", en la página 35.

Lectoras

Para habilitar verificación de una huella digital para una lectora SY-400:

Bajo la carpeta **Terminal list**, elija **SY-400**. El la lectora a ser conectada señale la casilla de verificación **Fingerprint**.

Para habilitar identificación de una huella digital para una lectora SY-400:

Paso 1. Bajo la carpeta **Terminal list**, elija **SY-400**. En la lectora a ser conectada señale la casilla de verificación **Fingerprint**.

Paso 2. En la misma pantalla elija lo siguiente **Reader Type [**Tipo de Lectora**]**: **Fingerprint Auto-Identification 10 digits** (debe ser be implementado solamente en la Lectora-1!)

Nota: *Para terminales SY-400, apenas una huella digital puede ser conectada a una de sus dos lectoras.*

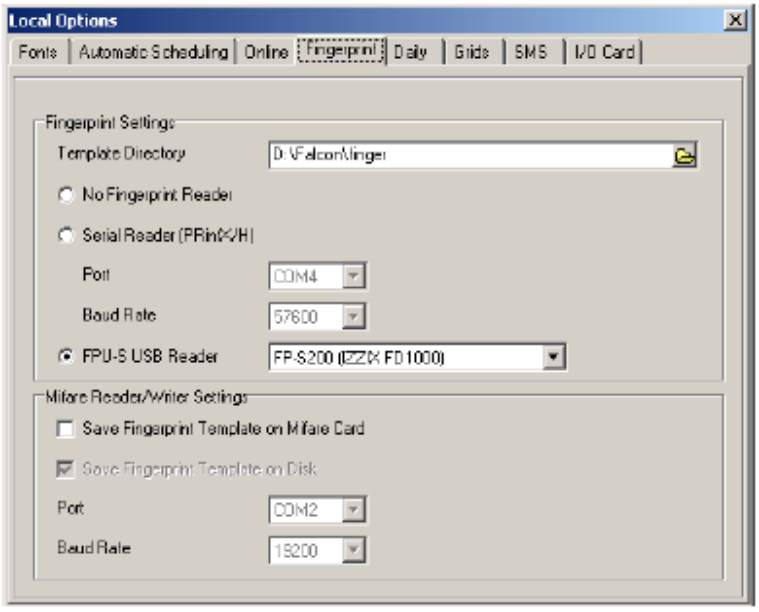
15.2 Software

15.2.1 Opciones del Sistema

Para información sobre definiciones sistemáticas de huellas digitales, véase el párrafo 3.3.2: "Configuraciones del Sistema ", en la página 10.

15.2.2 Opciones Locales

Bajo **Tools | Options | Fingerprint** usted puede establecer los parámetros de comunicación de la unidad de inscripción, como sigue:



Paso 1. Usted debe seleccionar el directorio que será usado para almacenar las plantillas de huellas digitales (en un entorno de usuarios múltiples, deberá ser colocado en un directorio compartido).

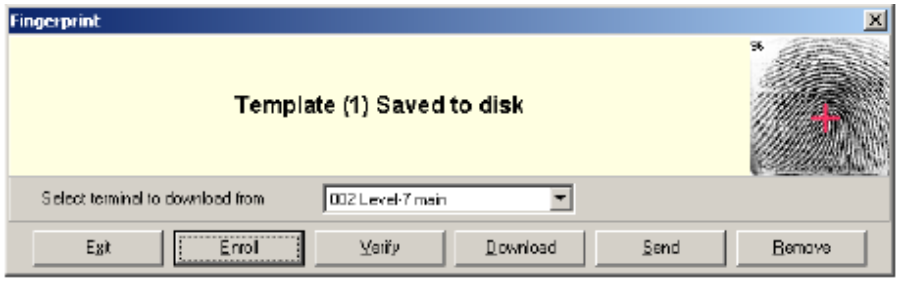
Paso 2. Seleccione la lectora de FP que está conectada a este PC.

Paso 3. Para una lectora serial, usted debe definir el **Port [**Puerto**]** (se recomienda usar un Puerto que no sea usado para fines de comunicación, de otro modo el usuario será forzado a trocar los cables manualmente), **Baud Rate [**Velocidad en baudios**]** (velocidad predeterminada de 57600).

Guardando a una Tarjeta Mifare

Falcon respalda dos tipos de inteligentes tarjetas sin contacto: Mifare-1KB y Mifare-4KB. Las huellas digitales pueden ser guardadas en estas tarjetas de manera segura, usándose la unidad de lectura/escritura Mifare. Cuando la casilla de verificación **Save FingerprintTemplate on Mifare Card [**Guardar la Plantilla de Huellas Digitales en la Tarjeta **Mifare]** está señalada, las plantillas inscritas serán guardadas en la tarjeta (con una opción para guardar una copia adicional en el disco). La verificación entonces será realizada solamente de la propia tarjeta.

15.2.3 Actividades del Empleado



Enroll [Registrar**]**

El registro es ejecutado como sigue:

Nota: *Para unidades a excepción de FPU-S usted puede registrar y verificar independientemente del tipo de unidad: verificación o identificación.*

Paso 1. En la pantalla **Personnel [**Personal**]** señale la fila relevante de empleado. Haga clic en el botón **Finger [**Dedo**]**.

Paso 2. Haga clic en **Enroll [**Registrar**]** en la pantalla **Fingerprint [**Huella Digital**]**. Aparece un mensaje instruyéndole para colocar su dedo.

Paso 3. Coloque su dedo en el dispositivo. Aparece un mensaje **Remove finger [**Remover dedo**]**.

Paso 4. Aparece un grado de la calidad de exploración (Véase calidad, contenido en el inicio de este capítulo).

Paso 5. En caso del usuario querer re-explorar, debe hacer clic en **No** y volver a la pantalla **Fingerprint**.

Paso 6. Si el usuario quiere confirmar, debe hacer clic en **OK**.

Paso 7. Al registrar en tarjetas Mifare:
Le van a pedir que aproxime su tarjeta, para guardar la plantilla de la lectora a la tarjeta.

Paso 8. Repetir los pasos 1-6 para cada plantilla.

Verify [Verificar**]**

Compara la plantilla guardada con el dedo que está actualmente colocado en la unidad.

Download [Descargar**]**

Elija el terminal relevante, después descargue las plantillas requeridas de aquel terminal. La descarga será realizada para el empleado (línea) resaltado. Es designado para:

- Registro desde el terminal y no desde el PC.
- Copia de Seguridad – Si la plantilla se perdió en el PC usted puede recuperarla del terminal.

Nota: *El programa registra todas las plantillas que fueron enviadas a un terminal. Después, durante la programación compara las plantillas y envía solamente las que no fueron enviadas. Es posible enviar todas las plantillas por medio de la pantalla* ***Communication***.

Send [Enviar**]**

Un archivo de plantilla del empleado puede ser enviado del PC a todos los terminales autorizados.

Remove [Quitar**]**

Un archivo de plantilla de empleado puede ser quitado del PC a todos los terminales autorizados (no del PC).

15.3 Sincronizando Plantillas

Bajo el menú **Maintenance [**Manutención**]** haga clic en **Synchronize Fingerprint Templates [**Sincronizar Plantillas de Huellas Digitales**]**. Esto hará con que el *Falcon* sincronice el directorio de huellas digitales: **Tools| Options| Fingerprint| Template directory** con el archivo de Personal del *Falcon*: *Falcon* explora el archivo del empleado y señala si hay para cada empleado un archivo de plantilla que corresponda.

Esto permite importar plantillas de huellas digitales desde un programa externo y hacer combinación cruzada con aquellas de una lista de empleados.

Capítulo 16 - Terminología

Anti-Pass Back **[**Contra Nueva Fichada**]** – Evita el múltiple acceso de una tarjeta condicionándola con una fichada en una segunda lectora en una distinta localización.

Auto Mode **[**Auto Modo**]** – Una opción de operación para la lectora que permite automáticamente cambiar los modos de trabajo según una Zona Horaria especificada. Estos modos son por ejemplo: solamente tarjeta, o tarjeta y PIN.

Camera site **[**Sitio de la cámara**]** – Un dispositivo o PC que es usado como un servidor para diversas cámaras.

Day Type **[**Tipo de Día**]** – Cuando la opción **Use Calendar [**Usar Calendario**]** está activa, usted puede definir un tipo de día: completo, medio día de trabajo, vacaciones, etc. (hasta 9).

Duress Code **[**Código de Amenaza**]** – Un código usado por un usuario amenazado por un intruso. Después de digitar este código la puerta se abre y simultáneamente un evento es enviado al equipo host. Usado por lectora de Acceso en el modo Tarjeta+PIN.

Employee ID **[**ID del Empleado**]** – Un número personal de ID para un empleado.

Expiry Date **[**Fecha de Caducidad**]** – La última fecha de validez de una tarjeta.

Event **[**Evento**]** – Una violación irregular de acceso registrada y exhibida en la pantalla **Online [**En Línea**]**.

Enroll **[**Registro**]** – Al usar la característica de huellas digitales, las huellas digitales del empleado son muestradas: El empleado coloca su dedo en la lectora, y el sensor explora el dedo.

Fire (report) **[**Despedir (informe)**]** – Permite emitir una lista de presencia actualizada.

Folder **[**Carpeta**]** – Once en número, representan las principales utilidades del software (módulos). Un clic en una carpeta exhibe cada pantalla de utilidad. (Presentadas desde el icono **Setup**/menú principal).

Local – Comunicación local (físicamente conectada), como RS232 y RS485

Map **[**Mapa**]** – Permite la presentación gráfica del croquis del terminal y de la lectora.

Padding – Un complemento de espacios de texto vacíos en un campo usando un dígito especial.

PEP File **[**Archivo PEP**]** – Directorios de proyecto para la unidad de control Com-II-PRO.

PIN – Un código personal como una medida suplementar de seguridad.

Reader **[**Lectora**]** – Una unidad de lectura.

Security Group **[**Grupo de Seguridad**]** – Un grupo a que fueron asignados parámetros especiales de seguridad

Terminal – Una unidad de control usada como un medio entre el PC y las lectoras.

Time Zone **[**Zona Horaria**]** – Define una zona horaria en la cual el acceso es permitido. Las Zonas Horarias son tipos de días definidos para el período de un año.

Verify **[**Verificar**]** – Confirmar el registro de la huella digital.

Identify **[**Identificar**]** – Comparar la huella digital registrada, con la huella digital almacenada en la memoria del terminal.

Capítulo 17 – Solución de Problemas

Bajo el menú **Help** | **About** | **Info** de *Falcon*, usted puede encontrar datos que serán útiles para el soporte técnico:

- Ruta de la Base de Datos
- Modo compartido local

<table>
<tr><th>Problema</th><th colspan="2">Como solucionar el Problema</th></tr>
<tr><td rowspan="5">Al enviar una configuración a un terminal Master un mensaje de error BCD (Bad Data Format [Mal Formato de Datos] es recibido del Phantom</td><td colspan="2">Debe ir a Terminal list | ficha Additions y verificar si el valor de Max. card ultrapasa su capacidad de Master:</td></tr>
<tr><td></td><td>Permitido</td></tr>
<tr><td>Master-128</td><td>2,976</td></tr>
<tr><td>Master-512 (P)</td><td>14,000</td></tr>
<tr><td>Master-512 (T-Special)</td><td>2,700</td></tr>
<tr><td>Después de la instalación no se puede abrir el Falcon o el administrador BDE</td><td colspan="2">Su presentación está configurada para 16 colores, en el panel de control cambie la presentación para un mínimo de 256 colores</td></tr>
<tr><td>No se puede imprimir ni ver en Vista Previa ningún informe</td><td colspan="2">Definir una impresora predeterminada en Windows</td></tr>
<tr><td>Las transacciones son colectadas pero no aparecen en la pantalla Online ni en los informes</td><td colspan="2">Cerciórese que el tipo de transacción en la lectora no está establecido como NONE.
Para Lectoras de Acceso: Setup| Terminal list| Master + Access| Access list|Access setup.
Para Lectoras SY-400: Setup| Terminal list| SY-400| Reader list| SY-400 Reader setup.</td></tr>
<tr><td>“El Índice no está actualizado”</td><td colspan="2">Una tabla se ha corrompido. Salga del Falcon y ejecute Reindex.exe del directorio Falcon mientras asegúrese de que nadie más esté usando el Falcon o la base de datos.
Para evitar este error:
1. Configure LOCAL SHARE como TRUE en todas las estaciones de trabajo.
2. Asegúrese que todas las estaciones de trabajo apuntan al mismo directorio compartido para la configuración de NET DIR, y que el alias del Falcon es exactamente lo mismo.</td></tr>
<tr><td>“El Directorio es controlado por otro archivo .NET”</td><td colspan="2">El programa terminó anormalmente y dejó archivos *.LCK y *.NET flotando. Cierre todos los programas BDE y busque y suprima los siguientes archivos en el servidor de archivo y en todas las estaciones de trabajo: PDOXUSRS.NET, PDOXUSRS.LCK, PARADOX.LCK
O, múltiples estaciones de trabajo accesando la misma tabla se están refiriendo a la NET DIR diferentemente. Cerciórese de que todas las estaciones de trabajo señalen al mismo directorio compartido para la configuración de la NET DIR, y que el alias del Falcon es exactamente lo mismo.</td></tr>
<tr><td>“Violación llave” mientras intentando guardar una nueva persona o colectar datos.</td><td colspan="2">La tabla Personnel (o Transactions) está corrompida, salga del Falcon (asegúrese que nadie más esté usando el Falcon o la base de datos) y del directorio Falcon ejecute ReIndex.exe con el símbolo de reparación \: c:\Falcon\ReIndex.exe /repair. Usted deberá ver un mensaje rojo “Repair option is ON” en la pantalla del programa ReIndex, presione el botón Start. (Por favor, antes haga copia de seguridad de su directorio de la base de datos!).</td></tr>
<tr><td>“El Directorio está ocupado.”</td><td colspan="2">Es posible que otro programa BDE esté usando el directorio privado del Falcon (predeterminado en el directorio TEMP del Windows). Por lo tanto es posible cambiar la ubicación del directorio privado del Falcon insertando un nuevo parámetro en el archivo Falcon.ini:
[General]
PrivateDir=x:\LocalPathName</td></tr>
</table>

Apéndice A – Integración CCTV (PRO)

El software del *Falcon* respalda la operación de cámara CCTV para visualización remota de las puertas de sus instalaciones.
Los siguientes sistemas CCTV son respaldados:

- Regard i y Regard Remote CS COM interfaz
- NegeVision VideoRemote
- Pelco matrix
- Vicon V1500 matrix

Regard: Regard i y Regard Remote CS COM interfaz

Los servidores de visión remota Regard ofrecen supervisión remota de video cámaras y otros aparatos. **Regard i** fue proyectado para atender a las necesidades de la industria de seguridad para control remoto de locaciones con hasta 8 cámaras fotográficas.

La visión de la cámara fotográfica es implementada a través de la red, así no se requiere conexión directa con el servidor de la cámara fotográfica.

Paso 1. Bajo Falcon.ini anote:
[Extensions]
EnableRegard=1

Paso 2. En la carpeta **Terminal List**, haga doble clic en el terminal relevante y anote lo siguiente:
Camera Site = el sitio como definido en Regard CS (Mayúsculas o minúsculas).
Camera Name = la cámara fotográfica como definida en la casilla Regard-i (Mayúsculas o minúsculas).

NegeVision: VideoRemote

El Video Server permite la administración de 4 cámaras fotográficas permitiendo control remoto de las localizaciones. Este servidor permite la integración entre el *Falcon* y un sistema CCTV.

La visión de la cámara fotográfica es implementada a través de la red, así no se requiere conexión directa con el servidor de la cámara fotográfica.

Paso 1. Bajo Falcon.ini anote:
[Extensions]
EnableRegard = 2

Paso 2. En la carpeta **Terminal List**, haga doble clic en el terminal relevante y anote lo siguiente:
Camera Site = Nombre o IP del servidor del Video Remote
Camera Name = el número de la cámara fotográfica en el servidor

Pelco: G-Protocol matrix

El *Falcon* respalda la visión multiplexor de la cámara fotográfica. Los multiplexores permiten visualizar corrientes de video de múltiplas cámaras fotográficas de supervisión a un solo sistema de visión. Requiere una conexión local de su PC a la matriz.

El *Falcon* soporta la familia de la matriz Pelco CCTV que opera en RS485 y los protocolos ‘G’. Es posible cambiar la cámara fotográfica activa en el monitor principal. Un monitor está conectado a la matriz y debe ser colocado adyacente a la pantalla del *Falcon*. El *Falcon* controla este monitor.

Paso 1. Bajo Falcon.ini anote:
[Extensions]
EnableRegard=3
MatrixPort=n
MaxricBaud=9600
“n” es el número del puerto COM designado: 1=COM1, 2=COM2 etc.

Paso 2. En la carpeta **Terminal List**, haga doble clic en el terminal relevante y anote lo siguiente:
Camera Site = ID de la unidad de la Matriz (generalmente 1 si hay una matriz)
Camera Name = el número de la cámara fotográfica en la matriz

Vicon: V1500

Soporte para el Vicon V1500 que opera en el protocolo RS-232. Este dispositivo tiene un intercambiador de matriz que permite conectar varias cámaras fotográficas a él y seleccionar una cámara fotográfica para ver a través de un monitor correspondiente. Un monitor debe ser colocado adyacente a la pantalla del *Falcon* para permitir visualizar datos en línea y el sitio simultáneamente. A través del *Falcon* usted puede determinar qué monitor corresponderá a qué cámara fotográfica.

Paso 1. Bajo Falcon.ini anote:
[Extensions]
EnableRegard=4
MatrixPort=n
MaxricBaud=9600
"n" es el número del puerto COM designado: 1=COM1, 2=COM2 etc.

Paso 2. En la carpeta **Terminal List**, haga doble clic en el terminal relevante y anote lo siguiente:
Camera Site = Número del monitor para mostrar la cámara fotográfica seleccionada
Camera Name = Número de la cámara fotográfica

Apéndice B – Base de Datos

Archivos

Access	Lista de lectoras de acceso
Auto4De	Auto Modo SY-400, detalle
Auto4Ma	Auto Modo SY-400, master
AutoDet	Auto-Modo Master, detalle
AutoMast	Auto-Modo Master, master
CLayout	Proyecto del croquis de la tarjeta
Com2Def	Definición del formato del Com-II-PRO
Company	Lista de la Compañía
CostCent	Lista del grupo de cálculo
Dates	Calendario definido por el usuario
DaysType	Tipos de día del calendario
Dept	Lista de departamentos
Detector	Lista de detectores de alarma
EvenTran	Transacciones de eventos todavía no cerrados
Events	Definición de evento
EvntHndl	Lista de respuesta predefinida para el tratamiento de evento
Formats	Formatos de transacciones (del Phantom.FMT)
GenParam	Parámetros generales
LuAuto	Lista de tipos de Auto-Modo para terminales Master
LuAuto4	Lista de tipos de Auto-Modo para terminales SY-400
LuCosTyp	Tipos de categoría de cálculo
LuEvent	Lista de tipos de Eventos
LuMoveTp	Lista de tipos de Transacciones (Ninguna, Entrada, Salida, Puerta)
LuPopTyp	Lista de tipos de Población (Regular, Visitante, Guardia)
LuRdrTyp	Lista de tipos de Lectoras SY-400 (Magnética, Código de Barras, etc.)
LuRunRel	Lista de modos de Operación del Relé SY-400 (Pulso, Set, Reset)
Maps	Definición de mapas
Messages	Todos los mensajes del software
MesSys	Mensajes del sistema
Objmap	Definición de ítems de los mapas
OldEvent	Transacciones cerradas de eventos (ya fueron tratadas)
PCardSnd	Actualizaciones acumuladas de tarjetas del Personal para ser enviadas a los terminales
PerCards	Asignación de tarjetas de Visitantes
PermCard	Lista de Personal
Persons	Lista de Visitantes
Reports	Informes definidos por el usuario (lista de los archivos *.REP)

Signal	Señalización de notificación de evento entre clientes
SY400Rdr	Lista de lectoras SY-400
TerGrDet	Grupos de seguridad, detalle
TerGrMas	Grupos de seguridad, master
Terminls	Lista de terminales
TimeZoDe	Zonas Horarias Master, detalle
TimeZoMa	Zonas Horarias Master, master
Transact	Todas las transacciones
TzSY4De	Zonas Horarias SY-400, detalle
TzSY4Ma	Zonas Horarias SY-400, master
Users	Lista de Operador
Week	Calendario predeterminado

Extensiones

Cada tabla consiste en uno o más de los siguientes archivos. Al copiar una tabla, cerciórese de copiar TODOS los archivos con el mismo nombre de base. Si los archivos de índice están faltando o corrompidos, use el programa Reindex.EXE para recrearlos.

*.DB	archivo base de datos, contiene todos los datos
*.MB	Archivo Memo, contiene campos grandes de notas
*.VAL	Chequeo de validez y valores predeterminados
*.PX	Índice primario
*.X??	Índices secundarios
*.Y??	Índices secundarios

Otros Archivos

*.REP – informes definidos por el usuario (instrucciones SQL)

Los siguientes archivos son parte del compartido Paradox y del esquema de cierre y serán creados automáticamente por el motor de la base de datos si aún no existen.

Si estos archivos salen de sinc, suprímalos y reinicie el *Falcon*.

PDOXUSRS.NET – archivo de control de la red Paradox
PDOXUSRS.LCK – archivo de cierre Paradox
PARADOX.LCK – archivo de cierre Paradox

Idiomas Extranjeros

La versión del *Falcon* inicialmente instalada es en inglés (véase el Capítulo 8, Traducción de mensajes): Si se requiere el respaldo de otro idioma se recomienda copiarlo de una fuente ya traducida. Utilice la utilidad FaLang.exe para traducir todas las tablas LU * (Véase Apéndice D – Utilidades).
Los siguientes archivos de base de datos pueden ser editados y copiados más adelante a otras instalaciones. Su localización predeterminada es C:\Falcon\DB.

DAYSTYPE.DB	DAYSTYPE.PX
LUAUTO.DB	LUAUTO.PX
LUAUTO4.DB	LUAUTO4.PX
LUCOSTYP.DB	LUCOSTYP.PX
LUEVENT.DB	LUEVENT.PX
LUMOVETP.DB	LUMOVETP.PX
LUPOPTYP.DB	LUPOPTYP.PX
LURDRTYP.DB	LURDRTYP.PX
LURUNREL.DB	LURUNREL.PX
MESSAGES.DB	MESSAGES.PX
MESSYS.DB	MESSYS.PX

Nota:

1. Al copiar los archivos de la base de datos (sufijo *.db) el archivo del índice equivalente (mismo nombre de sufijo*.px) debe también ser copiado.
2. Ejecute la copia solamente cuando el software del *Falcon* estuviera cerrado y ningún otro programa utilice estos archivos de base de datos

Apéndice C – Actualización

Para su atención: Se recomienda hacer copia de seguridad de su base de datos antes de actualizar el software.

Paso 1. Haga copia de seguridad de todo el directorio *Falcon*. Cerciórese de que hace copia de seguridad de los directorios locales y de red.
Anote la ruta de la DB del *Falcon* DB en el administrador BDE.

Paso 2. Al actualizar de una versión regular al PRO, suprima el archivo falcon.ini.

Paso 3. Copie la versión 2.23 del *Falcon* del directorio a su computadora en una carpeta provisoria (o obtenga la distribución del último CD).

Paso 4. Ejecute el setup.exe de la nueva versión. El procedimiento es similar a la instalación estándar. Cuando requerido, elija la ruta de la versión actual (i.e.: c:\Falcon).

Paso 5. Ejecute el Falcon.exe UNA VEZ del directorio del *Falcon* (un mensaje “Run again” aparece).

Paso 6. Vaya al administrador BDE y cerciórese que el alias apunta hacía la misma dirección como en el paso 1!

Paso 7. Ejecute FalcUpd.exe del directorio del *Falcon*.

Paso 8. Una ventana **Upgrade to Falcon 2.23 [**Actualizar para Falcon 2.23**]** aparece. Usted puede aceptar la opción predeterminada, y pasar al paso 10 o:

Paso 9. Elegir la versión de donde está actualizando. Usted puede también elegir un alias distinto o un directorio diferente donde su actual (versión antigua) instalación de la DB está ubicada.

Paso 10. Haga clic en **Stara [**Iniciar**]**. Después de actualizar, un mensaje **Upgrade successful [**Actualizado con éxito**]** aparece. Cierra la ventana **Upgrade [**Actualizar**]**.

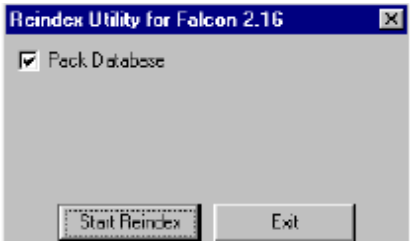
Paso 11. Ejecute el Falcon.exe y cerciórese de que el procedimiento de actualización a sido completado con éxito.

Paso 12. Al actualizar de versiones más antiguas que 2.19 usando el SY-400, usted debe reprogramar los terminales. Si está usando un SAL especial para su programación, cerciórese de que es compatible con la versión actualizada del *Falcon*.

Apéndice D – Utilidades

La siguientes utilidades externas están incluidas en la instalación del *Falcon*:

ReIndex.exe

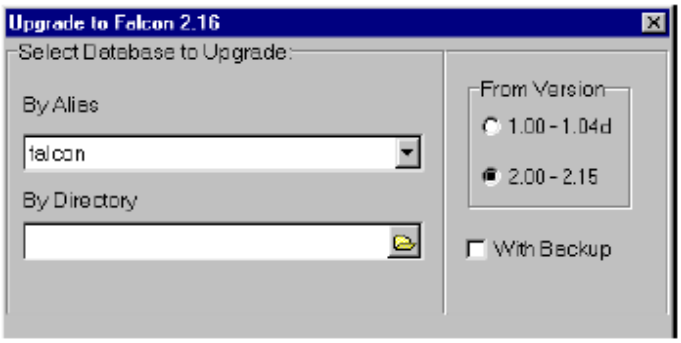


Crea archivos de índice del *Falcon*. Use este programa cuando el *Falcon* no puede cargar debido a un archivo de índice corrompido, deteriorado o en falta.

Este programa también puede **Pack [**Empaquetar**]** la base de datos a fin de mejorar la estructura interna de la DB y ahorrar el espacio de registros eliminados.

Permite transacciones de reparación y tablas autorizadas bajo: c:\Falcon\ReIndex.exe /repair. Haga copia de seguridad de su base de datos antes de activar el procedimiento de reparación!

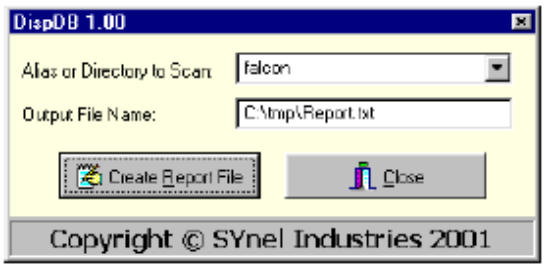
FalcUpd.exe



Actualiza la base de datos del Falcon a partir de una versión antigua. Véase el Apéndice C – Actualización.

Estas utilidades opcionales pueden ser encontradas en el CD del *Falcon* bajo el directorio **Utility [**Utilidad**]**:

DispDb.exe



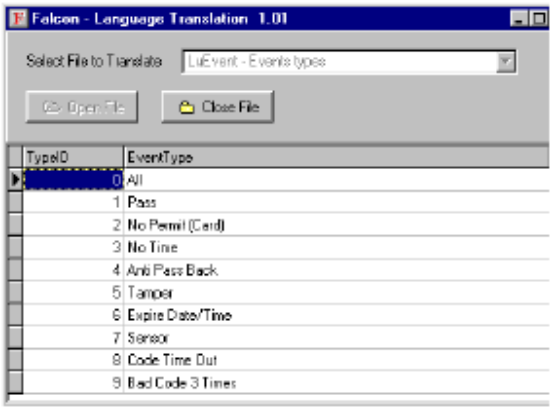
Crea un archivo de texto con una lista completa de la estructura de la base de datos Paradox (Requiere *Falcon* 2.14 o superior a ser instalado en la computadora).

FalDel.exe

Elimina un grupo de personas de la lista de personal del *Falcon* según reglas definidas.

FalLang.exe

Permite al usuario traducir y editar tablas de utilidad usadas por el *Falcon*.



Apéndice E – Configuración de la Red Master

Usar el Master en la comunicación de red puede ser implementado como sigue:
Cuando su PC y las máscaras de subred son idénticos, la configuración del Ethernet Master es hecha usándose un programa **Telnet**. Al usar una máscara de subred diferente, usted puede:

1. Cambiar la dirección IP de su PC para ser compatible con la máscara de la subred Master (por ejemplo: 192.168.0.10) y después usar Telnet o:
2. Usar el protocolo ARP para permitir acceso a los comandos de Telnet y después configurar el IP requerido del Master (solamente a partir de la versión 4.5 de CoBox!).

***Nota**: Para que el comando ARP funcione en **Windows**, la tabla ARP en el PC debe tener por lo menos una dirección IP definida a parte de la suya propia. Si la tabla ARP está vacía, el comando devolverá un mensaje de error. Introduzca ARP -A a continuación del símbolo del sistema DOS para verificar que haya por lo menos una entrada en la tabla ARP.*
Si la PC local es la única entrada, 'ping' otra dirección IP en su red para construir una nueva entrada en la tabla ARP; la dirección IP debe ser un host a parte de la PC en la cual usted está trabajando.

La nueva dirección IP predeterminada del Master es 192.168.0.2

Nota: *Para evitar conflicto de IP cerciórese de que ningún otro dispositivo comparte su dirección IP:*
- Desconecte el cable Ethernet del Master.
- 'Ping' al IP del Master o al IP predeterminado del nuevo terminal.
- Si la dirección IP es confirmada, alguien está utilizando esta dirección y usted no puede utilizarla para el Master.
- si esta dirección IP es rechazada, conecte el Master y reintente 'pinging'.
- En el caso de que el IP del Master es confirmado, usted puede hacer la configuración usando Telnet:

Procedimientos Telnet:

- Abra Telnet en el menú **Start** | **Run** del Windows, y escriba:
  telnet terminal-IP-address 9999
- La dirección y versión del dispositivo servidor MAC aparece. Presione **Enter**.
- Los parámetros básicos del dispositivo son exhibidos (véase la tabla abajo).

Parámetro	Valor	Comentario
Baudrate	9600	
I/F Mode	4C	
Flow	00	
Porto No.	3734	En Windows XP el puerto 5000 puede estar ocupado por otro programa. Elija un puerto distinto
Connect Mode	C0	
Remote IP	0.0.0.0	
Disconnmode	00	
FlushMode	A0	
Pack Cntrl	00	
DisConnTime	00:10	
SendChar 1	00	
SendChar 2	00	

Usted debe elegir la configuración relevante:

0 – Configuración del Servidor – Se refiere a la dirección IP
1 – Configuración del Canal 1 – Se refiere a la configuración de la comunicación
5 – Configuraciones Avanzadas – Se refiere al recomendado intervalo de actualización de la red
6 – Seguridad – No cambie
7 – Predeterminados en fábrica – No cambie
8 – Salir sin guardar
9 – Guardar y salir

- Teclee 1 y Enter.

De la versión 4.5 de la tarjeta master ethernet

- Teclee 5 (para configuraciones avanzadas) + Enter
- Cambie “TCP keepalive time in s” para 45
- Teclee 9 para guardar y salir

De la versión 5.1ab de la tarjeta master ethernet

- Teclee 5 (para configuraciones avanzadas) + Enter
- Cambie “TCP keepalive time in s” para 45
- Cambie “ARPcheck timeout in s” para 30
- Teclee 9 para guardar y salir

Usando el Comando ARP

Para usar los comandos de configuración IP ARP usted debe conocer la dirección del Ethernet MAC (Empiece del párrafo 5). Si usted no sabe la dirección MAC haga lo siguiente:

1. Abra la tapa del terminal.
2. Retire la tarjeta Ethernet y apunte la dirección MAC (indicada en una etiqueta adhesiva), i.e: 00-20-4A-54-5A-12.
3. Conecte la tarjeta Ethernet.
4. Conecte el Master a su red local o al HUB que se conecta a la PC que usted quiere usar.
5. Use el menú **Start | Run** del Windows o el **Command Prompt** y ejecute run “arp -s (Nuevo IP) (dirección MAC)”
6. Ejecute Telnet (nuevo IP) puerto 1.
7. Ejecute Telnet según los procedimientos de Telnet.
8. Intente comunicarse usando la nueva dirección.

Ejemplo de ARP:
Dirección del terminal MAC: 00-20-4A-54-5A-12
IP requerido: 192.168.2.128
Formato de los comandos debe ser:
arp -s 192.168.2.128 00-20-4A-54-5A-12
telnet 192.168.2.128 1
Cuando un mensaje de “Connection failure” aparece - ignórelo!
telnet 192.168.2.128 **9999**
Editar 0 – configuración del Servidor
Cambie la dirección IP del Master al nuevo IP.
Ejecute Telnet según los procedimientos de Telnet.
Guarde y salga.

Apéndice F – Mensajes de Error

Origen	Parámetro	Solución
Mensajes del Sistema (Borland)	"El índice no está actualizado"	Una tabla se ha corrompido. Salga del *Falcon* y ejecute Reindex.exe del directorio Falcon mientras asegúrese de que nadie más esté usando el *Falcon* o la base de datos. Para evitar este error: 1. Configure LOCAL SHARE como TRUE en todas las estaciones de trabajo. 2. Asegúrese que todas las estaciones de trabajo apuntan al mismo directorio compartido para la configuración de NET DIR, y que el alias del *Falcon* es exactamente lo mismo.
	"El Directorio es controlado por otro archivo .NET"	El programa terminó anormalmente y dejó archivos *.LCK y *.NET flotando. Cierre todos los programas BDE y busque y suprima los siguientes archivos en el servidor de archivo y en todas las estaciones de trabajo: PDOXUSRS.NET, PDOXUSRS.LCK, PARADOX.LCK O, múltiples estaciones de trabajo accesando la misma tabla se están refiriendo a la NET DIR diferentemente. Cerciórese de que todas las estaciones de trabajo señalen al mismo directorio compartido para la configuración de la NET DIR, y que el alias del Falcon es exactamente lo mismo.
	"Violación llave" mientras intentando guardar una nueva persona o colectar datos.	La tabla Personnel (o Transactions) está corrompida, salga del Falcon (asegúrese que nadie más esté usando el *Falcon* o la base de datos) y del directorio Falcon ejecute ReIndex.exe con el símbolo de reparación \: c:\Falcon\ReIndex.exe /repair. Usted deberá ver un mensaje rojo "Repair option is ON" en la pantalla del programa ReIndex, presione el botón Start. (Por favor, antes haga copia de seguridad de su directorio de la base de datos!).
Mensajes del *Falcon*	Falla en la confirmación – La contraseña de la confirmación no combina con la nueva contraseña!	Operador o contraseña no válidos. Anote los detalles del operador y la contraseña correctos.
	Contraseña incorrecta – Acceso denegado.	Es imposible operar el programa pues una contraseña inválida fue anotada varias veces.
	Validación del número de la tarjeta – la extensión de la tarjeta es igual a 0	Un número de tarjeta debe ser asignado a cada empleado.
	Validación del número de la tarjeta – El número de la tarjeta debe contener apenas dígitos!	Un número de tarjeta no debe contener letras, marcas, símbolos o espacios. Debe consistir solamente de dígitos.
	Número de tarjeta duplicado - Incapaz de fijar.	Existe un número de tarjeta único para cada empleado. Anote otro número (o verifique si el número que usted acaba de anotar está asignado a otro empleado).
	Error del Phantom	Error durante la operación del Phantom. Para más información refiérase a la lista de mensajes del Phantom.
	Iniciando Exploración en Línea –Ningún terminal activo ha sido seleccionado para esta operación	La casilla de verificación **Participate in online scan [**Participar de Exploración en Línea**]** no está señalada en ningún terminal de la lista de terminales. Por favor, señale los terminales relevantes, según sus requisitos.
	Puerto erróneo - Abrir Puerto	En la pantalla **Terminal setup [**Configuración del Terminal**]** bajo **Communication** defina un puerto existente /disponible.

Origen	Parámetro	Solución
	Programación – Error al crear tablas	Verifique la ruta del directorio del proyecto en la pantalla **General Parameter [**Parámetros Generales**]** bajo **Files and Directories [**Archivos y Directorios**]**. Entonces, cerciórese de que existe tal directorio y que el usuario tiene acceso a ese directorio. Además, verifique que para todos los terminales SY-400 bajo la ficha **Additions [**Adiciones**]**, la ruta del **Project directory [**Directorio del Proyecto**]** está correcta.
	Ningún terminal fue seleccionado para esta operación	En el sistema no fueron definidos terminales activos o ningún terminal fue marcado en la pantalla **Communication**
	Por favor envíe **Permitted [**Permitido**]** desde la pantalla **Communication.**	**Personnel**| **Send Last [**Personal | Enviar el Último**]** es respaldado solamente por terminales Master. Para SY-400 hay que esperar la próxima actualización.
	Valor no válido de Fecha / Hora	Bajo **Communication** anote la fecha válida antes de enviar datos al terminal.
	El informe no existe!	Un informe almacenado anteriormente por el generador de informes no puede ser emitido. Es posible que la configuración del informe haya sido calculada erróneamente. Defina nuevamente los parámetros del informe usando el generador de informes.
	Terminal no definido	Como la tabla del grupo de seguridad está corrompida, fue registrado el tipo erróneo de terminal; elimine esta fila y agregue una nueva fila si requerido.
	Hasta 255 terminales pueden ser definidos!	No es posible añadir un nuevo terminal a la lista de terminales. Por favor, refiérase a un representante de Synel para expansión del sistema según sus requerimientos.
	Archivo no encontrado!	El archivo o el programa no existen.
	Error!	Un mensaje general de error generalmente seguido por una descripción general del problema (texto en Ingles).
	Error al guardar imagen en el disco!	¡Cerciórese de que el usuario tenga permiso para Escribir en la carpeta **Pictures** (Imágenes) y que no existe una carpeta **Pictures** de solo lectura, inducida por el sistema!
	El archivo no puede ser abierto / creado!	Verifique la localización del archivo de exportación: si el alias es a un directorio existente en el cual el usuario tiene permiso para Escribir. Cerciórese de que el archivo no esté ocupado por otro proceso.
	La tabla esta vacía!	Nada más para eliminar, la tabla está vacía!
	Registro no encontrado!	Elija un orden diferente (nombre, ID etc.) o quizá el empleado no existe.
	Error al abrir la tabla!	Error al publicar el informe **Message [**Mensaje**]**, reintente emitir el informe. Si el problema persiste refiérase a Synel.
	Archivo usado por otro usuario! No se puede reindexar ahora	Probablemente l archivo está ocupado por otro programa/usuario. Salga de todos los programas que se refieren a la base de datos del *Falcon* y después intente volver a reindexar.
	Error al crear informe!	Generalmente sigue un texto en Ingles, indicando la razón. Informe el texto específico al equipo de soporte técnico de Synel.
	Primero cierre **Preview [**Vista Previa**]**!	Hay una ventana abierta/minimizada de la pantalla Preview. Por favor, ciérrela e intente entrar nuevamente al programa.
	Error al exportar archivo!	El archivo no puede ser exportado. Anote nombres válidos para el archivo y el directorio para el archivo de exportación.

Apéndice G – Servidor SY

Para realizar chequeos en línea, el *Falcon* usa un Servidor SY como un programa de comunicación. El Servidor SY utiliza un DLL compatible que verifica los datos de entrada y los escribe en la base de datos del *Falcon.*

Para instalar el Servidor SY usted debe referirse a la documentación relevante o a su departamento de soporte técnico.

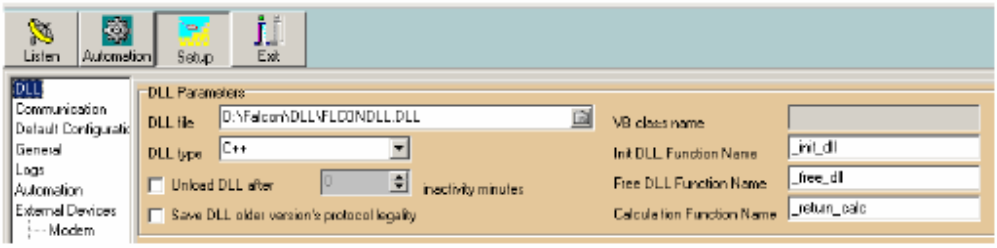
Después de haber instalado el Servidor SY, usted debe:

- Configurar las definiciones del Servidor SY
- Configurar las definiciones del *Falcon*
- Configurar las definiciones DLL

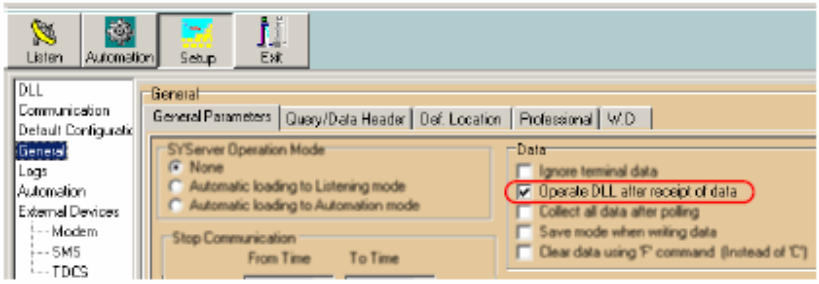
Definiciones del Servidor SY

Cambie las configuraciones según las pantallas que siguen:

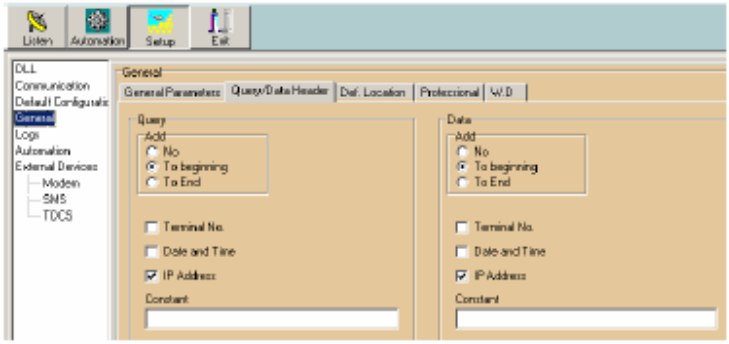
1.



2. El parámetro señalado, que es el único parámetro relevante en la siguiente pantalla, debe ser señalado.



3. Bajo **Setup** | **General**, defina sus configuraciones de **Query/Data Header** como sigue:



Definiciones Falcon

1. En la pantalla parámetros del terminal SY-400:
   - Bajo **Additions** anote un valor más grande que 0 bajo **Automatic Data Send Freq**. (el valor recomendado es entre 1-10 segundos).
   - Bajo **FPU** usted debe determinar el modo FPU, para permitir la validación en línea de huellas digitales (para huellas que no están almacenadas en la memoria de los terminales).
2. En la pantalla parámetros de la lectora SY-400 | **Validation**:
   Señale la casilla de verificación **Host**. Si la lectora participa en **Global APB**, señale también esta casilla de verificación.
3. En **General Parameters | Communication** señale **Write Last Transaction into Personnel File** (usada para chequeos Global APB).

Definiciones DLL

Bajo **Utility\SySrv400.dll** en su CD del *Falcon* usted encontrará dos variaciones del mismo DLL:
1. FlconDLL.dll – Operación DLL estándar
2. FlconDBG.dll – Lo mismo que el DLL estándar, y además registra todas las actividades en el archivo debug.dat.

Para ajustar su DLL estándar, usted puede editar las siguientes secciones en el archivo FlconDLL.ini:
- Validación del número de la tarjeta (incluyendo la zona horaria por grupo de seguridad)
- APB Global
- Grupo de Cálculo
- SyGina (Cerradura de Seguridad del PC)
- Tarjetas Robadas